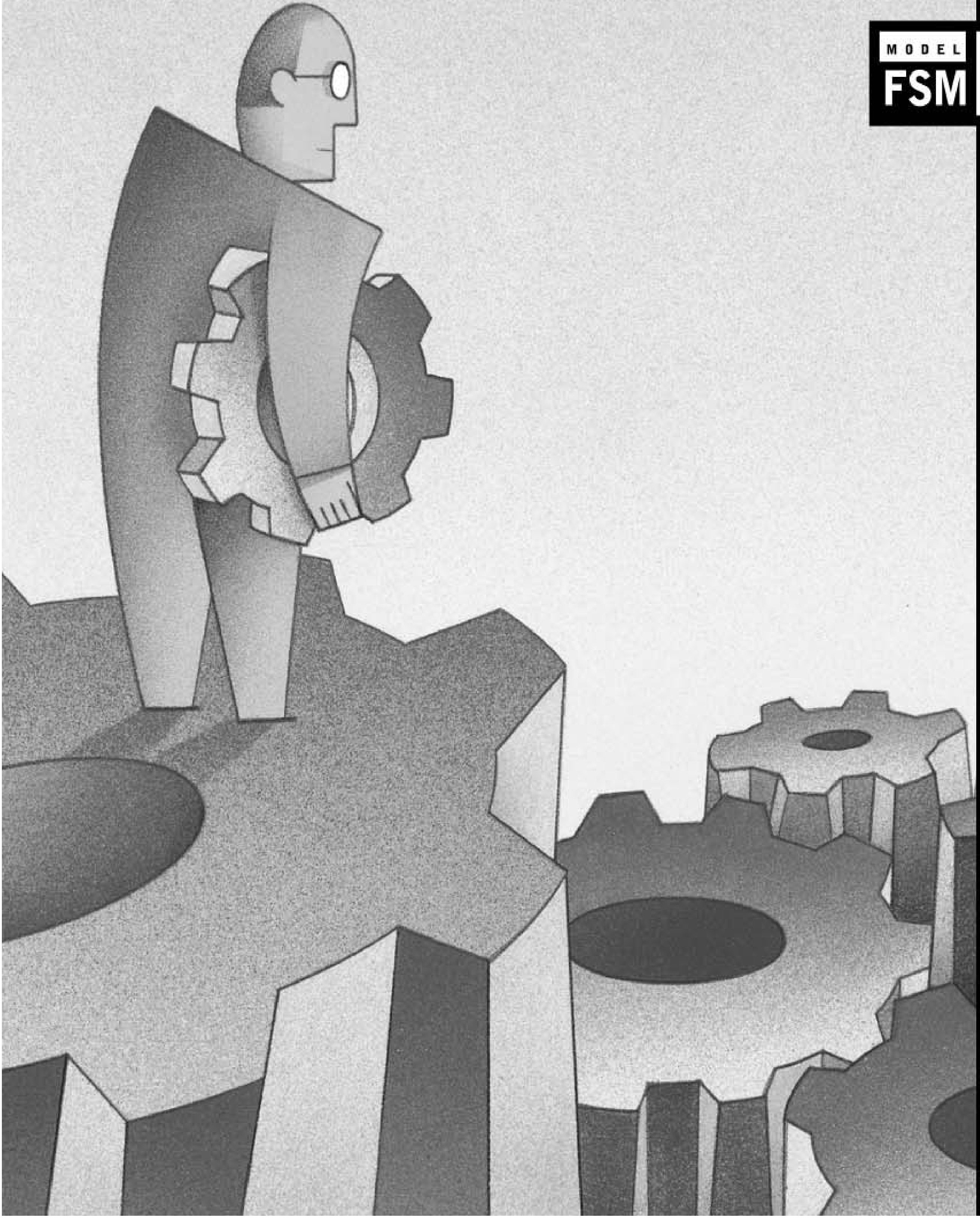
NETGEAR®

26 PORT 10/100/1000 Mbps

Managed Stackable Switch

Installation Guide

MODEL FSM 726S



Trademarks

NETGEAR® is a registered trademark of NETGEAR, Inc. in the United States and other countries. Auto Uplink™ is a trademark of NETGEAR, Inc. All other trademarks and registered trademarks are the property of their respective owners.

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, NETGEAR reserves the right to make changes to the products described in this document without notice. NETGEAR does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Certificate of the Manufacturer/Importer

It is hereby certified that the NETGEAR Model FSM726S Managed Stackable Switch has been suppressed in accordance with the conditions set out in the BMPT-AmtsblVfg 243/1991 and Vfg 46/1992.The operation of some equipment (for example, test transmitters) in accordance with the regulations may, however, be subject to certain restrictions. Please refer to the notes in the operating instructions.

Federal Office for Telecommunications Approvals has been notified of the placing of this equipment on the market and has been granted the right to test the series for compliance with the regulations.

Voluntary Control Council for Interference (VCCI) Statement

This equipment is in the first category (information equipment to be used in commercial and/or industrial areas) and conforms to the standards set by the Voluntary Control Council for Interference by Data Processing Equipment and Electronic Office Machines that are aimed at preventing radio interference in commercial and/or industrial areas.

Consequently, when this equipment is used in a residential area or in an adjacent area thereto, radio interference may be caused to equipment such as radios and TV receivers.

Federal Communications Commission (FCC) Compliance Notice: Radio Frequency Notice

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

This device may not cause harmful interference.

This device must accept any interference received, including interference that may cause undesired operation.

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

Reorient or relocate the receiving antenna.

Increase the separation between the equipment and receiver.

Connect the equipment into an outlet on a circuit different from that which the receiver is connected.

Consult the dealer or an experienced radio/TV technician for help.

EN 55 022 Declaration of Conformance

This is to certify that the NETGEAR Model FSM726S Managed Stackable Switch is shielded against the generation of radio interference in accordance with the application of Council Directive 89/336/EEC, Article 4a. Conformity is declared by the application of EN 55024 Class A (CISPR 22).

EN 55 022 and EN 55 024 Statements

This is to certify that the NETGEAR Model FSM726S Managed Stackable Switch is shielded against the generation of radio interference in accordance with the application of Council Directive 89/336/EEC, Article 4a. Conformity is declared by the application of EN 55 022 Class A (CISPR 22) and EN 55 024.

⚠ Warning: This is a Class A product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take appropriate measures.

Canadian Department of Communications Radio Interference Regulations

This digital apparatus (NETGEAR Model FSM726S Managed Stackable Switch) do not exceed the Class A limits for radio-noise emissions from digital apparatus as set out in the Radio Interference Regulations of the Canadian Department of Communications.

Règlement sur le brouillage radioélectrique du ministère des Communications

Cet appareil numérique (NETGEAR Model FSM726S Managed Stackable Switch) respecte les limites de bruits radioélectriques visant les appareils numériques de classe A prescrites dans le Règlement sur le brouillage radioélectrique du ministère des Communications du Canada.

Customer Support

For assistance with installing and configuring your NETGEAR system or with questions or problems following installation:

- Check the NETGEAR Web page at http://www.NETGEAR.com.
- Call Technical Support in North America at 1-888-NETGEAR. If you are outside North America, please refer to the phone numbers listed on the Support Information Card that shipped with your switch.
- Email Technical Support at support@NETGEAR.com.

Defective or damaged merchandise can be returned to your point-of-purchase representative.

Internet/World Wide Web

NETGEAR maintains a World Wide Web home page that you can access at the uniform resource locator (URL) http://www.NETGEAR.com. A direct connection to the Internet and a Web browser such as Internet Explorer or Netscape are required.

CONTENTS

Figures

Tables

CHAPTER 1: INTRODUCTION

Congratulations on your purchase of the NETGEAR Model FSM726S Managed Stackable, Fast Ethernet Switch! Your NETGEAR Switch is a state-of-the-art, high-performance, IEEE-compliant network solution designed for users who require a large number of ports and want the power of management to eliminate bottlenecks, boost performance, and increase productivity. In addition to providing easy, straightforward management, your switch is expandable and comes with two stacking ports that can connect to other NETGEAR Model FSM726S Managed Stackable Switches. Additionally, your switch provides flexible Gigabit speed connections to servers and other Gigabit Ethernet switches. There are two Gigabit Ethernet ports on the switch that can be used either by the built-in RJ-45 ports or by the Gigabit Interface Converter (GBIC) module bays, both located on the front panel. To simplify installation, the switch is shipped ready for use. Everything necessary for setup comes in the box.

This chapter serves as the introduction for using your NETGEAR FSM726S Stackable Switch and provides the following information:

Overview

Switch Features

Package contents

Overview

Your NETGEAR Model FSM726S Managed Stackable Switch provides the benefit of management with a complete package of features for the observation, configuration, and control of your network. With a web-based Graphical User Interface (GUI), the switch's many capabilities can be viewed and used in a simple and intuitive manner. For those who prefer a more traditional interface, there is a Command Menu Interface available through the console port on the front. The switch's management features include SNMP and RMON for port and switch information, VLAN for traffic control, port trunking for increased bandwidth, and Class of Service (CoS) for traffic prioritization. These features and more will allow you to better understand and better control your network.

Your NETGEAR Model FSM726S Managed Stackable Switch includes two bi-directional stacking ports, which can connect to other NETGEAR Model FSM726 Manageable Switches. This built-in stackability gives you the flexibility to buy the number of ports you need now to meet your immediate needs, then add ports to your system later as your networking requirements grow.

Your NETGEAR Model FSM726S Managed Stackable Switch also provides two Gigabit Ethernet ports that are used either by the built-in RJ-45 ports or by the GBIC module bays, both located on the front panel. The GBIC module bays will accept any standard GBIC module, including the AGM721F 1000BASE-SX module from NETGEAR. Using these Gigabit ports, you can create high-speed connections to a server or network backbone. For example, you can:

- Connect switches to each other with high-speed links
- Link up to high-speed servers
- Connect fiber and copper networks

Your NETGEAR Model FSM726S Managed Stackable Switch can be free-standing, or rack mounted in a wiring closet or equipment room. It is IEEE-compliant and offers low latency for high-speed networking. It includes 24 auto-sensing 10/100 Ethernet/Fast Ethernet ports. The 10/100 ports are shielded RJ-45 ports that automatically negotiate to the highest speed. This capability makes the switch ideal for environments that have a mix of Ethernet and Fast Ethernet devices. In addition, all 10/100 Mbps ports operate in half- or full-duplex mode, increasing the maximum bandwidth of each connection up to 20 Mbps or 200 Mbps, respectively. The maximum segment length is 328 feet (100 meters) over Category 5 unshielded twisted-pair (UTP) cable.

Features

The following list identifies the key features of the NETGEAR Model FSM726S Managed Stackable Switch.

- Twenty-four 10/100 Mbps auto sensing Fast Ethernet switching ports
- Two Gigabit Ethernet ports that can be used either through the built-in RJ-45 ports for 10/100/1000 Mbps connectivity or through the GBIC modules for a variety of fiber connections
- Two, built-in gigabit speed stacking ports for network expandability and scalability up to six stacked units
- Full Layer 2 switch management including:
    - SNMP
    - RMON (groups 1,2,3 and 9)
    - IEEE 802.1Q (up to 64 Static VLAN groups)
    - IEEE 802.1p (Class of Service)
    - IEEE 802.1ad (Link Aggregation)
    - IEEE 802.1D (Spanning Tree)
    - IGMP snooping
    - Port Mirroring
    - Password access control
    - TFTP firmware upgrade
    - Multiple interfaces: Browser-based, Telnet, or SNMP application
- Full compatibility with IEEE standards:
    - IEEE 802.3i, (10BASE-T)
    - IEEE 802.3u (100BASE-TX)
    - IEEE 802.3ab (1000BASE-T)
    - IEEE 802.3x (full-duplex flow control)
- Auto-sensing and auto-negotiating capabilities for all ports
- Auto Uplink™ on all ports to make the right connection
- Automatic address learning function to build the packet-forwarding information table. The table contains up to 8,000 media access control (MAC) addresses (that is, the switch can support networks with as many as 8,000 devices).
- Full- and half-duplex functions for all 10/100 ports
- Store-and-Forward transmission to remove bad packets from the network
- Active flow control to minimize packet loss/frame drops:
    - Half-duplex back-pressure control
    - Full-duplex IEEE 802.3x pause frame flow control
- LED indicators for port status monitoring:
    - Power LED to indicate power on/off status
    - Link LED to indicate link status and activity
    - Dual-color Mode LED to indicate speed, activity, duplex mode, and collision
    - Stacking LED to indicate link status, activity, and master/slave status
- Easy migration from existing 10 Mbps network to 100 Mbps Fast Ethernet network
- Easy upgrade path to add gigabit technology to your network
- Flexible installation:
    - Standalone desktop installation
    - 19-inch standard rack-mount
- Standard 1U case size

Package Contents

Figure 1-1 shows the package contents of the NETGEAR Model FSM726S Managed Stackable Switch.

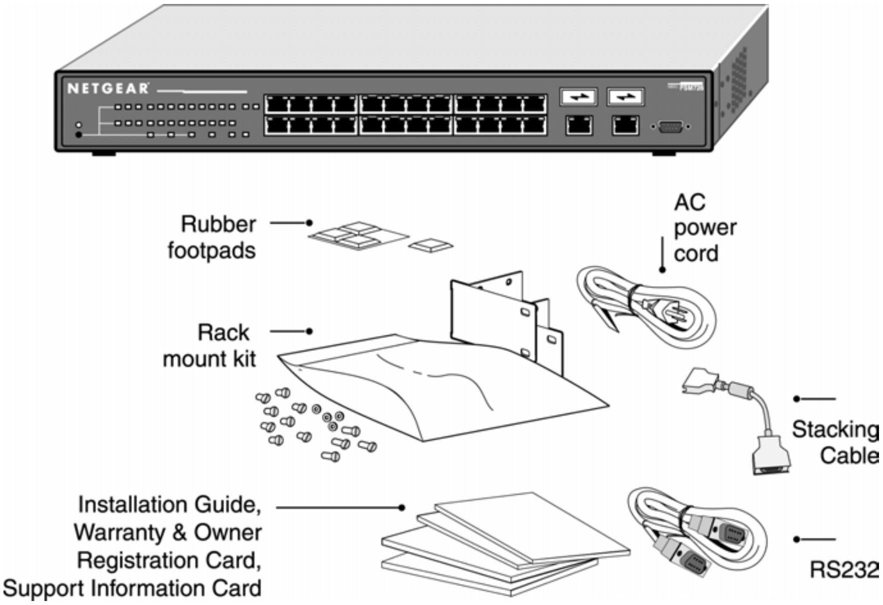

NETGEAR
Rubber footpads
AC power cord
Rack mount kit
Stacking Cable
Installation Guide, Warranty & Owner Registration Card, Support Information Card
RS232

Figure 1-1. Package Contents

Verify that your package contains the following:

One FSM726S Managed Stackable Switch

Rubber footpads for tabletop installation

Power cord

One null-modem cable

One stacking cable

Rack-mount kit for installing the switch in a 19-inch rack

This user’s guide

Support Information Card

Warranty & Owner Registration Card

If you ordered additional GBIC modules with your switch, they are provided in a separate package.

If any item is missing or damaged, contact your place of purchase immediately.

CHAPTER 2: PHYSICAL DESCRIPTION

This chapter describes the hardware features of the NETGEAR Model FSM726S Managed Stackable Switch. Topics include:

Front and back panels

10/100 Mbps auto-sensing RJ-45 ports

Gigabit Ethernet Ports (RJ-45 and GBIC module bay)

LED descriptions

Console port

Stacking ports

Front Panels

Figures 2-1 and 2-2 show the key components on the front and back panels of the NETGEAR Model FSM726S Managed Stackable Switch.

The front panel contains LEDs, RJ-45 jacks, GBIC module bays, and a console port. The back panel has two stacking ports and a standard AC power receptacle for accommodating the supplied power cord.

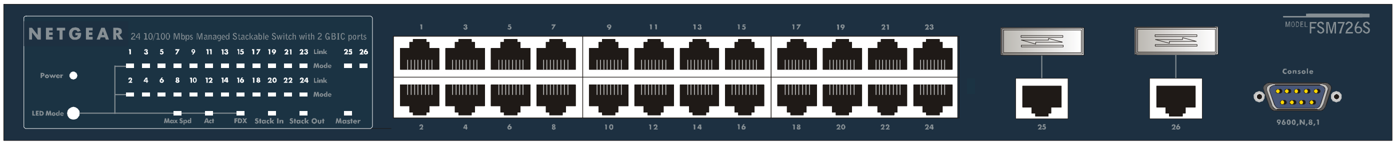

NETGEAR
24 10/100 Mbps Managed Stackable Switch with 2 GBIC ports
1 3 5 7 9 11 13 15 17 19 21 23 Link 25 26
Mode
2 4 6 8 10 12 14 16 18 20 22 24 Link
Mode
Power
LED Mode
Max Spd
Act
FDX
Stack In
Stack Out
Master
MODEL FSM726S
Console
9600,N,8,1

Figure 2-1. Front Panel of the FSM726S Managed Stackable Switch

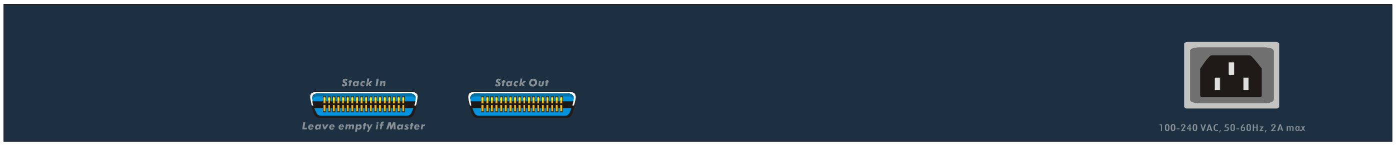


Figure 2-2. Back Panel of the FSM726S Managed Stackable Switch

10/100 Mbps RJ-45 Ports

As Figure 2-1 shows, the FSM726S Managed Stackable Switch has 24 10/100 Mbps RJ-45 ports. These ports are auto-sensing 10/100 Mbps ports: When you insert a cable into an RJ-45 port, the switch automatically ascertains the maximum speed (10 or 100 Mbps) and duplex mode (half- or full-duplex) of the attached device. The 10/100 Mbps ports support only unshielded twisted-pair (UTP) cable terminated with an 8-pin RJ-45 plug.

To simplify the procedure for attaching devices, all RJ-45 ports support Auto Uplink. This technology lets you attach devices to the RJ-45 ports using either straight-through or crossover cables. When you insert a cable into the switch's RJ-45 port, the switch automatically:

- Senses whether the cable is a straight-through or crossover cable, and
- Determines whether the link to the attached device requires a "normal" connection (such as when connecting the port to a PC) or an "uplink" connection (such as when connecting the port to a router, switch, or hub).
- After ascertaining this information, the switch automatically configures the RJ-45 port to enable communications with the attached device, without requiring user intervention. In this way, the Auto Uplink technology compensates for setting uplink connections, while eliminating concern about whether to use crossover or straight-through cables when attaching devices.

Warning! You must use Link Aggregation (a.k.a. Port Trunking) to create multiple links between switches. Using Auto Uplink to create multiple active paths between any two network devices can cause undesirable loops in the network, resulting in an endless broadcast traffic that disables your network. Loops occur when there are alternate routes between two network devices. In Figure 2-3, for example, a loop is created by connecting two RJ-45 ports on a NETGEAR Model FSM726S Managed Stackable Switch to a router containing a 4-port switch. The Spanning Tree protocol will prevent loops, if that advanced feature is enabled.

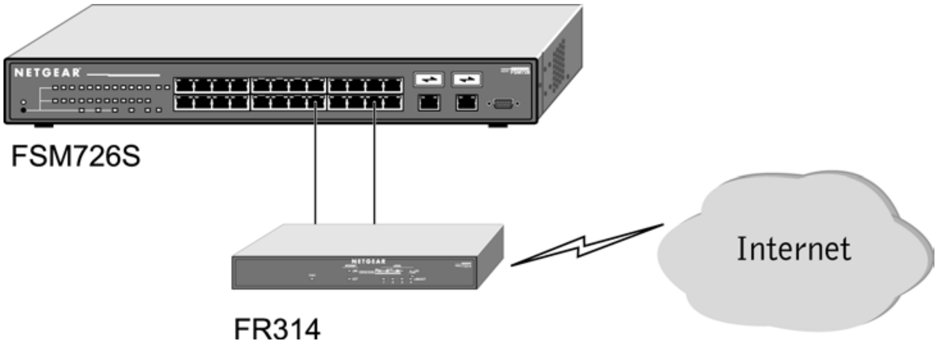


Figure 2-3 Creating Redundant Paths between Network Devices

Gigabit Ethernet Ports (RJ-45 and GBIC module bay)

Your NETGEAR Model FSM726S Managed Stackable Switch has two Gigabit Ethernet ports that can be used as either a 1000BASE-T port or as a GBIC module bay. The default setting for port 25 and port 26 is for the built-in RJ-45 connector to be active, but they can be independently configured to activate either the RJ-45 or the GBIC module, enabling multiple combinations of fiber and copper connections. The Gigabit Ethernet ports provide a full-duplex 1000 Mbps (1 Gbps) connection that effectively doubles throughput to 2 Gbps.

The GBIC bay accommodates a standard GBIC module, such as the NETGEAR AGM721F 1000BASE-SX GBIC module. This module has an SC connector that is compatible with the IEEE 802.3z 1000BASE-SX standard.

LED Descriptions

The front panel of the NETGEAR Model FSM726S Managed Stackable Switch has LEDs that provide a quick and accurate display of port speed, activity, collisions, and duplex mode. For stacked use, there are additional LEDs for link status and master unit status (to indicate master/slave status in a stack). The Gigabit Ethernet ports also have LEDs that show link and mode status. Table 2-1 summarizes the LEDs on the switch and Gigabit Ethernet module.

Table 2-1. Front Panel LEDs:

Label	Color	Activity	Description
Power	Green	On	Power is supplied to the switch.
	Yellow	On	Power On Self Test (POST) in progress
		Blinking	Hardware failure during POST
		Off	Power is disconnected
Link	Green	On	Port has a valid link connection.
(the port number)		Off	A valid link has not been established on the port.
LED Mode in (Three LEDs)			
Max Spd	Green	On	Port has made a connection at the fastest speed possible for that port. For 10/100 Mbps ports, it indicates a 100 Mbps connection. For a 10/100/1000 Mbps port, it indicates a 1 Gbps connection.
		Off	Port is not operating at the fastest speed possible.
ACT	Green	Blinking	Data transmission is occurring on the port.
		Off	No data transmission is occurring on the port.
FDX	Green	On	Port is operating in full-duplex mode.
	Yellow	On	Port is operating in half-duplex mode.
		Blinking	Collision is occurring.
Stack In	Green	On	Stack In port has a valid link connection.
		Off	Stack In port does not have a valid link connection
Stack Out	Green	On	Stack Out port has a valid link connection.
		Off	Stack Out port does not have a valid link connection
Master	Green	On	Switch acts as a master unit in a stack of FSM726S switches.
		Off	Switch acts as a slave unit in a stack of FSM726S switches.

Console Port

Your NETGEAR Model FSM726S Managed Stackable Switch has a console port on the front panel. This port is labeled **Console** and is **required for initial configuration** of the switch. It also lets you manage the switch using a directly connected VT-100 terminal, personal computer (PC), Apple Macintosh, or UNIX workstation. The terminal, computer, or workstation connects to the console port using the null-modem cable supplied with your switch.

The console port is configured to use the following settings:

- Baud rate: 9,600 bps
- Data bits: 8
- Parity: none
- Stop bit: 1
- Flow control: none

These settings appear below the connector on the switch front panel.

In addition to using the console port, you can manage the switch using a Web browser and/or a Simple Network Management Protocol (SNMP) management program.

Note: You must use the console port for the initial switch configuration.

For more information about console-port connections, see “Connecting to the Console Port” on page 20. For more information about managing the switch, see Chapter 5.

Stacking Ports

Your NETGEAR Model FSM726S Managed Stackable Switch has two stacking ports on the back panel, each with a full-duplex throughput of 2.6 gigabit per second (Gbps). These ports are labeled **Stack In** and **Stack Out**. You can use the stacking ports to cascade NETGEAR Model FSM726S Managed Stackable Switches as your network grows to a maximum of six FSM726S Switches. The front panel of the switch contains **Stack In** and **Stack Out** LEDs that show link on these stacking ports. For more information about stacking switches, see “Connecting Switches to the Stack’s Backplane” on page 19.

CHAPTER 3: APPLICATIONS

Your NETGEAR Model FSM726S Managed Stackable Switch is designed to provide flexibility in configuring your network connections. It can be used as stand-alone devices or used with 10 Mbps, 100 Mbps, 10/100 Mbps, and 1000 Mbps hubs and switches. It can also be stacked with other FSM726S Switches to create one large virtual switch. This chapter shows how the switch can be used in various network environments.

Topics include:

Desktop switching

Stacked Switching

Desktop Switching

Your NETGEAR Model FSM726S Managed Stackable Switch can be used as desktop switch to build a small network that enables users to have 1000 Mbps access to a file server. With full-duplex enabled, the switch port connected to the server or PC can provide 2000 Mbps throughput.

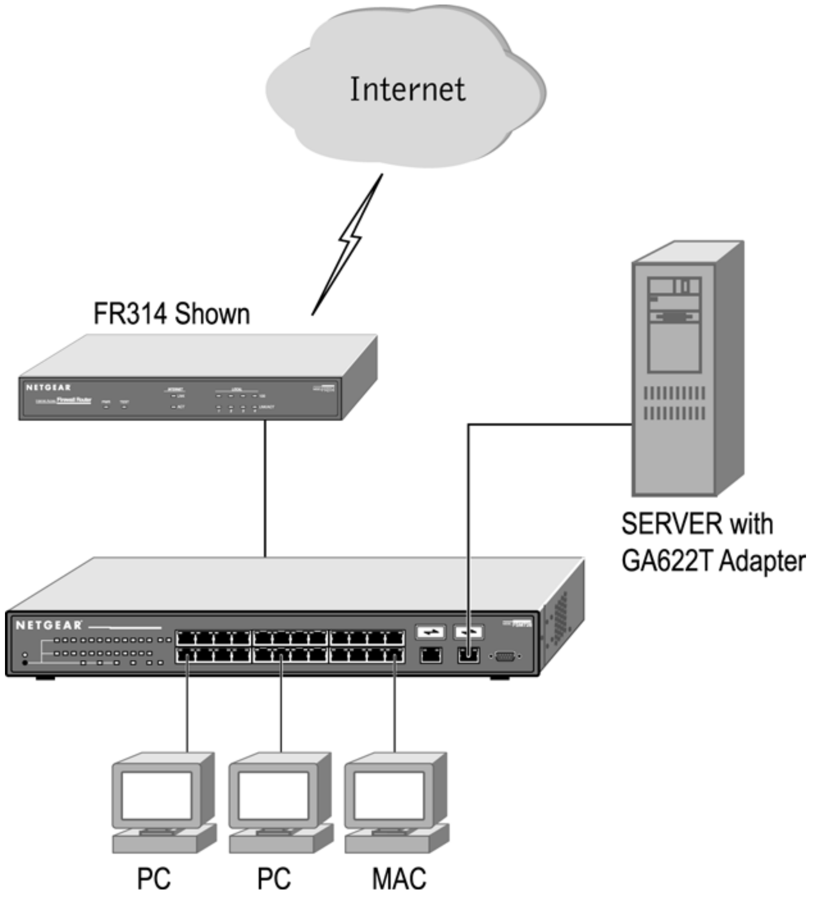


Figure 3-1. Example of Desktop Switching

Stacked Switching

Your NETGEAR Model FSM726S Managed Stackable Switch has two bi-directional stacking ports on the back panel. Using these ports, you can build a full-duplex, switched network for large numbers of users simply by stacking units together. The high-speed stacking ports deliver 2 Gbps of throughput across the stacking backplane.

A total of 6 switches can be put into a single stack. Stacked FSM726S Managed Stackable Switches can be assigned a single IP address using the switch's management software. The stack can then be treated as a single manageable unit with one IP address.

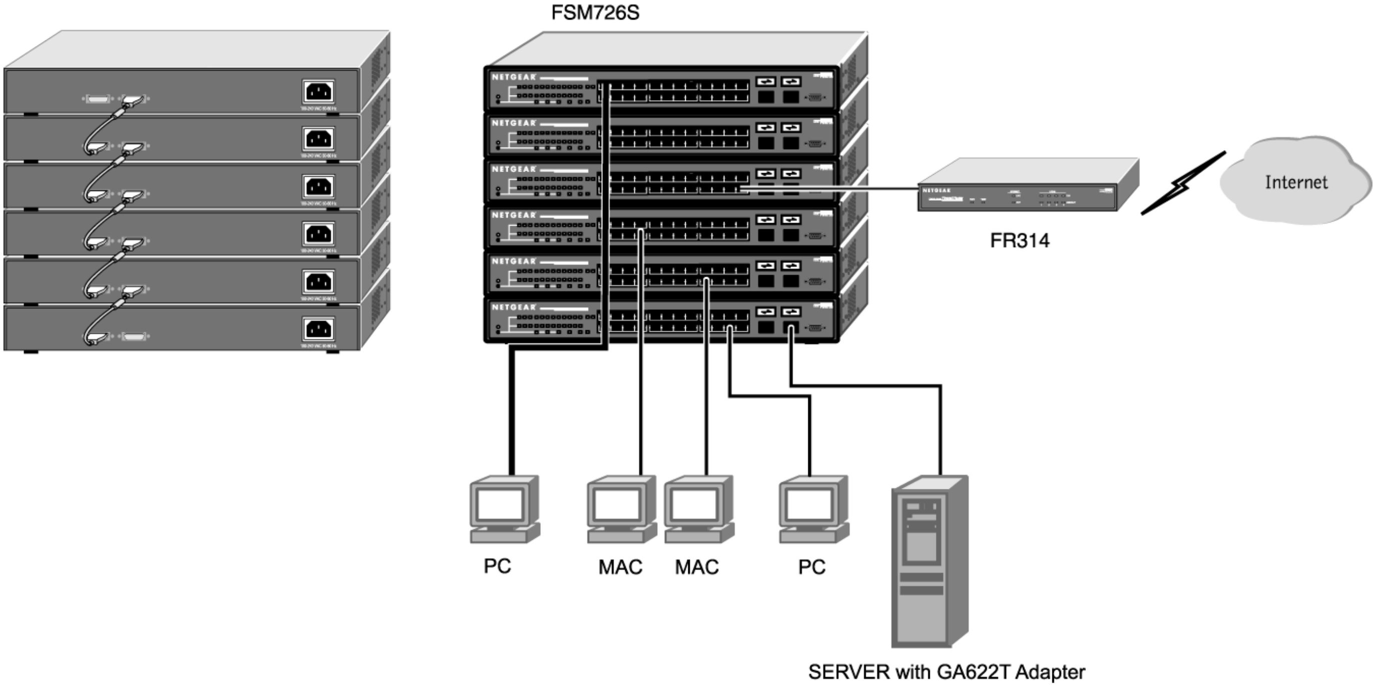


Figure 3-2. Example of Switched Stacking

CHAPTER 4: INSTALLATION

This chapter describes the installation procedures for your NETGEAR Model FSM726S Managed Stackable Switch. Switch installation involves the following steps:

Step 1: Preparing the site

Step 2: Installing the switch

Step 3: Installing a GBIC module Connecting devices to the switch

Step 4: Connecting Switches to the Stack's Backplane

Step 5: Checking the installation

Step 6: Applying AC power

Step 7: Connecting to the console port to manage the switch (initial configuration)

Step 8: Connecting devices to the switch

This chapter also discusses how to add or remove switches to your stack

Step 1: Preparing the Site

Before you install your switch, be sure your operating environment meets the operating environment requirements in Table 4-1.

Table 4-1. Site Requirements

Characteristics	Requirements
Mounting	
Desktop installations:	Provide a flat table or shelf surface.
Rack-mount installations:	Use a 19-inch (48.3-centimeter) EIA standard equipment rack that is grounded and physically secure. You also need the rack-mount kit supplied with your switch.
Access	Locate the switch in a position that lets you access the front panel RJ-45 ports, view the front panel LEDs, and access the rear-panel stacking port(s) and power connector.
Power source	Provide a power source within 6 feet (1.8 meters) of the installation location. Power specifications for the switch is shown in Appendix C. Be sure the AC outlet is not controlled by a wall switch, which can accidentally turn off power to the outlet and the switch.
Environmental	
Temperature:	Install the switch in a dry area, with ambient temperature between 0 and 40ºC (32 and 104ºF). Keep the switch away from heat sources such as direct sunlight, warm air exhausts, hot-air vents, and heaters.
Operating humidity:	The installation location should have a maximum relative humidity of 90%, non-condensing.
Ventilation:	Do not restrict airflow by covering or obstructing air inlets on the sides of the switch. Keep at least 2 inches (5.08 centimeters) free on all sides for cooling. Be sure there is adequate airflow in the room or wiring closet where you intend to install the switch.
Operating conditions:	Keep the switch at least 6 ft (1.83 m) away from nearest source of electromagnetic noise, such as a photocopy machine.
Stacking	If you intend to stack two or more switches, be sure the mounting surface can safely support the switch stack. Also, be sure there is adequate space around the stack for ventilation and cooling.

Step 2: Installing the Switch

You can install your NETGEAR Model FSM726S Managed Stackable Switch on a flat surface or in a standard 19-inch rack.

Installing the Switch on a Flat Surface
The switch ships with four self-adhesive rubber footpads. Stick one rubber foot pad on each of the four concave spaces on the bottom of the switch. The rubber footpads cushion the switch against shock/vibrations. They also provide space between each stacked switch for ventilation.

Installing the Switch in a Rack

To install the switch in a rack, use the following procedure (and refer to Figure 4-1). To perform this procedure, you need the 19-inch rack-mount kit supplied with your switch.

1. Attach the supplied mounting brackets to the side of the switch.
2. Insert the screws provided in the rack-mount kit through each bracket and into the bracket mounting holes in the switch.
3. Tighten the screws with a #1 Phillips screwdriver to secure each bracket.
4. Align the mounting holes in the brackets with the holes in the rack, and insert two pan-head screws with nylon washers through each bracket and into the rack.
5. Tighten the screws with a #2 Phillips screwdriver to secure the switch in the rack.
6. If you want to install a GBIC module, proceed to “Step 3: Installing a GBIC Module,” next. If you want to stack switches, proceed to “Step 4: Connecting Switches to the Stack’s Backplane,” Otherwise, skip to “Step 5: Checking the Installation.”

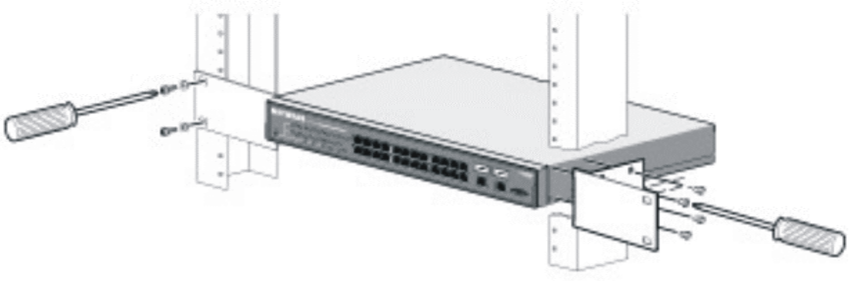


Figure 4-1. Attaching Mounting Brackets

Step 3: Installing a GBIC Module

The following procedure describes how to install a GBIC Gigabit Ethernet module, such as the NETGEAR AGM721F, in the switch’s Gigabit module bays. The AGM721F is sold separately from the FMS726S. If you do not want to install a GBIC module at this time, skip this procedure.

To install a GBIC module:

7. Insert the GBIC module into the GBIC module bay. Press firmly to ensure the module seats into the connector.
8. After the switch has been powered on, use one of the management interfaces (web browser or console interface) to configure the Gigabit Ethernet port with the GBIC module installed to the GBIC option.
9. To install a second Gigabit Ethernet module, repeat this procedure using the second module and the unoccupied module bay.
10. If you want to stack switches, proceed to “Step 4: Connecting Switches to the Stack’s Backplane,” next. Otherwise, skip to “Step 5: Checking the Installation.”

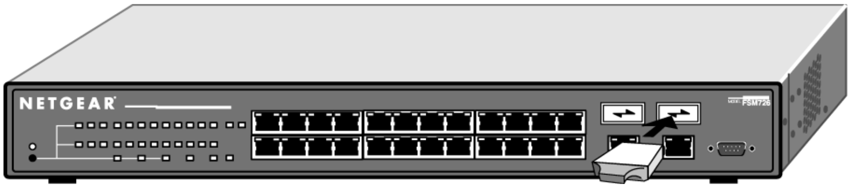


Figure 4-2. Installing a Gigabit Ethernet Module

Step 4: Connecting Switches to the Stack’s Backplane

Your NETGEAR Model FSM726S Managed Stackable Switch provides two stacking connectors. You can use these connectors to cascade up to six switches together to create one large virtual switch (for more information, see “Stacked Switching” on page 17).

Observe the following guidelines when installing the switches in a stacked configuration.

Connecting Stacking Ports
When connecting two FSM726S Managed Stackable Switches, one stacking cable connects the stacking port on one switch to the stacking port on the other switch.

Connect Straight-in
To prevent bent pins, do not install the stack port cable connector at an angle. Use extra care to insert the cable connector straight into the switch's stacking connector.

The following procedure describes how to stack three FSM726S Managed Stackable Switches and Figure 4-3 shows these connections:

11. Connect either end of the supplied stacking cable to the Stack In connector on the first switch. Connect the other end of the cable to the Stack Out connector on the second switch.
12. Connect either end of another stacking cable to the Stack In connector on the second switch. Connect the other end of the cable to the Stack Out connector on the third switch. The third switch will be the master switch.

Note: Stacked FSM726S Switches can be assigned a single IP address using the switches' management software. The stack can then be treated as a single manageable unit with one IP address. The switch with that IP address is considered the master unit, while the other switches in the stack are called slave units.

Note: The switch that is acting as the master unit should have the **Stack In** port empty.

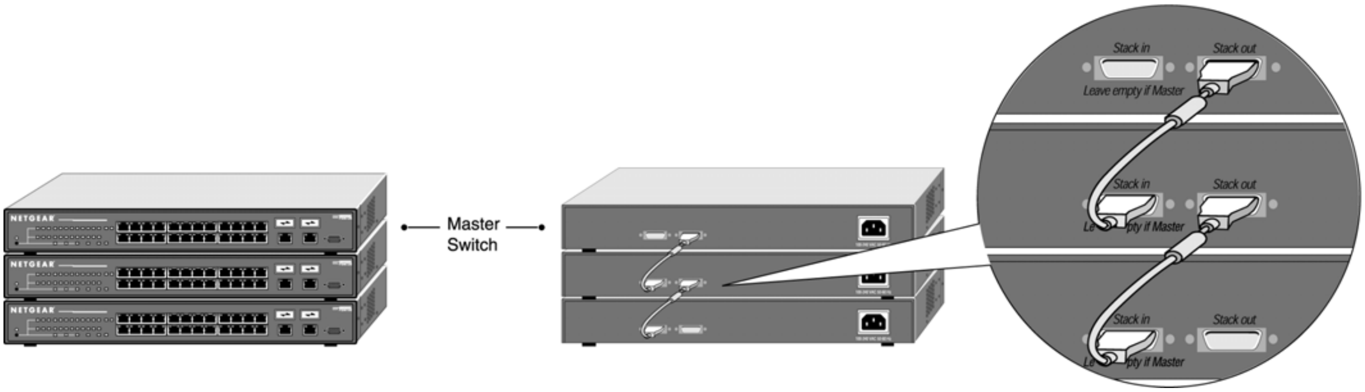


Figure 4-3. Cabling Three FSM726S Stacked Switches

Step 5: Checking the Installation

Before you apply power:

- Inspect the equipment thoroughly.
- Verify that all cables are installed correctly.
- Check cable routing to make sure cables are not damaged or create a safety hazard.
- Be sure all equipment is mounted properly and securely.

Step 6: Applying AC Power

NETGEAR Model FSM726S Managed Stackable Switches do not have an ON/OFF switch; the only method of applying or removing AC power is by connecting or disconnecting the power cord. Before you connect the power cord, select an AC outlet that is not controlled by a wall switch, which can turn off power to the switch. After you select an appropriate outlet, use the following procedure to apply AC power.

13. Connect the female end of the supplied AC power adapter cable to the power receptacle on the back of the switch.
14. Connect the 3-pronged end of the AC power adapter cable to a grounded 3-pronged AC outlet.

When you apply power, the **Power** LED on the switch's front panel will be Yellow, as it conducts a Power On Self Test (POST). After the switch passes the POST, the **Power** LED will change to Green and the switch is functional and ready to pass data.

If the **Power** LED does not go on, check that the power cable is plugged in correctly and that the power source is good. If this does not resolve the problem, refer to Appendix B, Troubleshooting.

Note: If you are powering up stacked FSM762 switches, power up the master unit last.

Step 7: Connecting to the Console Port to Manage the Switch (initial configuration)

Your NETGEAR Model FSM726S Managed Stackable Switch contains software for viewing, changing, and monitoring the way it works. This management software is not required for the switch to work. You can use the 10/100 Mbps ports, the built-in RJ-45 Gigabit ports, and the stacking ports without using the management software. However, the management software can let you improve the efficiency of the switch and, as a result, improve its overall performance as well as the performance of your network. The remainder of this section describes how to initialize the management software to the first time you use the management features.

After you power-up the switch for the first time, you can configure it using a VT100/ANSI terminal or a PC, Apple Macintosh, or UNIX workstation that is directly connected to the switch's console port. Thereafter, you can assign an IP address, subnet mask, and gateway address to the switch and manage it through a Web browser, Telnet session, or SNMP management application. For more information about using the console, see Chapter 6, Administration Console Access.

To connect a console to the switch:

15. Connect a VT100/ANSI terminal or a PC, Apple Macintosh, or UNIX workstation to the switch's console port, labeled Console, using the null-modem cable supplied with the switch. The supplied null-modem cable has 9-pin connectors on each end.

Note: you must connect the console cable to the master switch. Connecting the console cable a slave switch will not allow configuration

Note: If you are stacking your switches, you only have to configure the Master unit via the Console port. Once you have assigned an IP address to the master unit, you can use the browser interface to configure the other units.

16. If you attached a PC, Apple Macintosh, or UNIX workstation, start a terminal-emulation program.

    Microsoft Windows users can use HyperTerminal, which comes with the Windows operating systems.

    Macintosh users can use ZTerm.

    UNIX users can use a terminal emulator such as TIP.

17. Configure the terminal-emulation program to use the following settings:

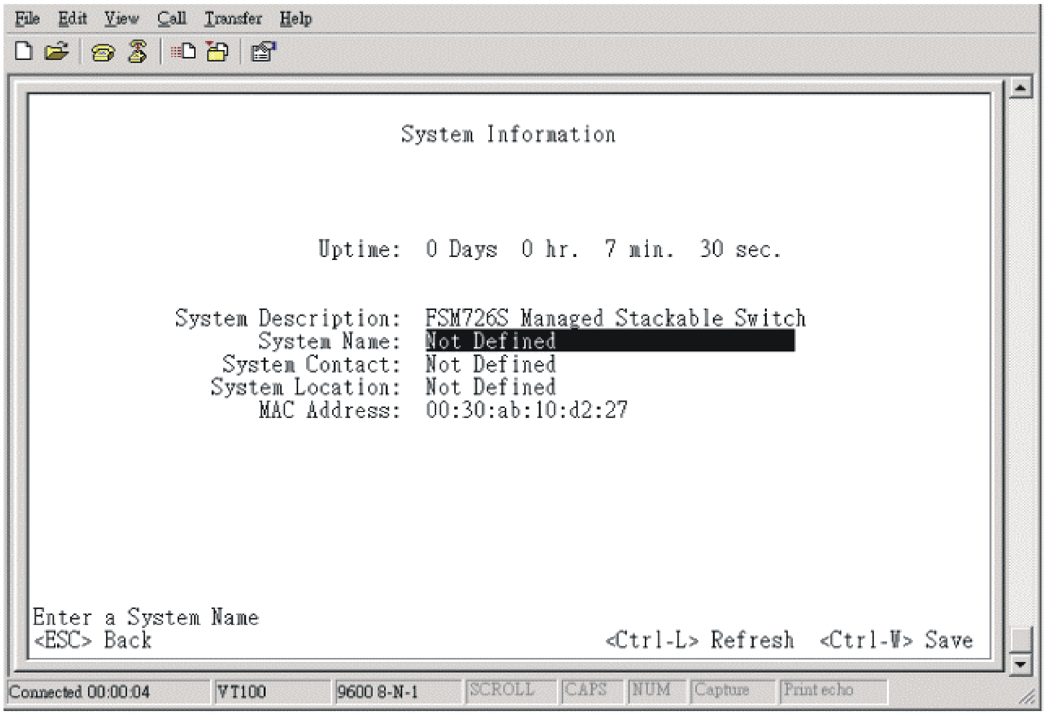
    Baud rate: 9,600 bps

    Data bits: 8

    Parity: none

    Stop bit: 1

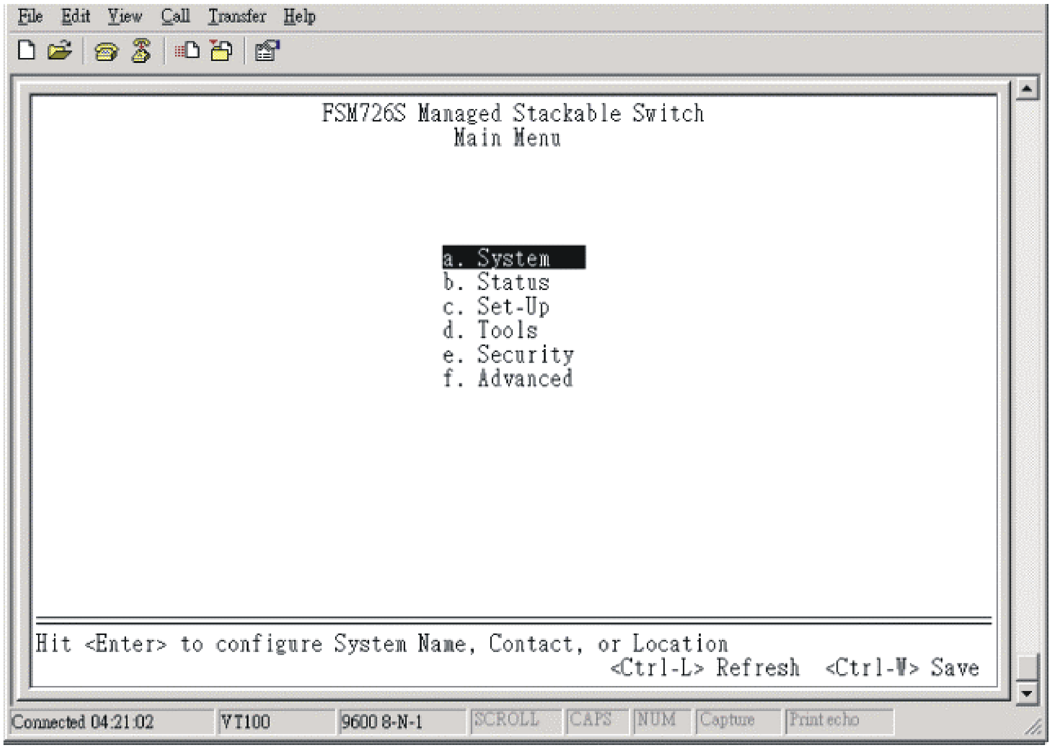
    Flow control: none



```
                         System Information



                 Uptime:  0 Days  0 hr.  7 min.  30 sec.


     System Description:  FSM726S Managed Stackable Switch
            System Name:  Not Defined
         System Contact:  Not Defined
        System Location:  Not Defined
            MAC Address:  00:30:ab:10:d2:27





Enter a System Name
<ESC> Back                                 <Ctrl-L> Refresh  <Ctrl-W> Save
```

Figure 4-4 System Description

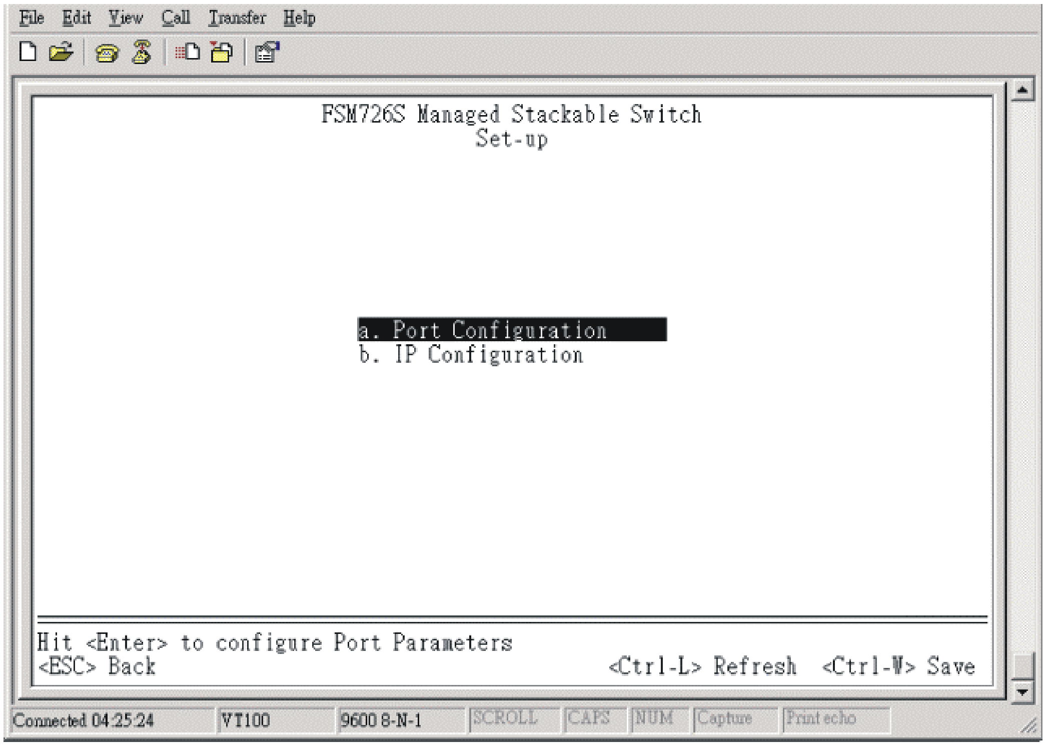
18. The terminal-emulation program should display the System Description page. Hit the ‘ESC’ key to get to the Main Menu page.



```
                FSM726S Managed Stackable Switch
                           Main Menu




                          a. System
                          b. Status
                          c. Set-Up
                          d. Tools
                          e. Security
                          f. Advanced








Hit <Enter> to configure System Name, Contact, or Location
                                      <Ctrl-L> Refresh  <Ctrl-W> Save
```

Figure 4-5 Main Menu

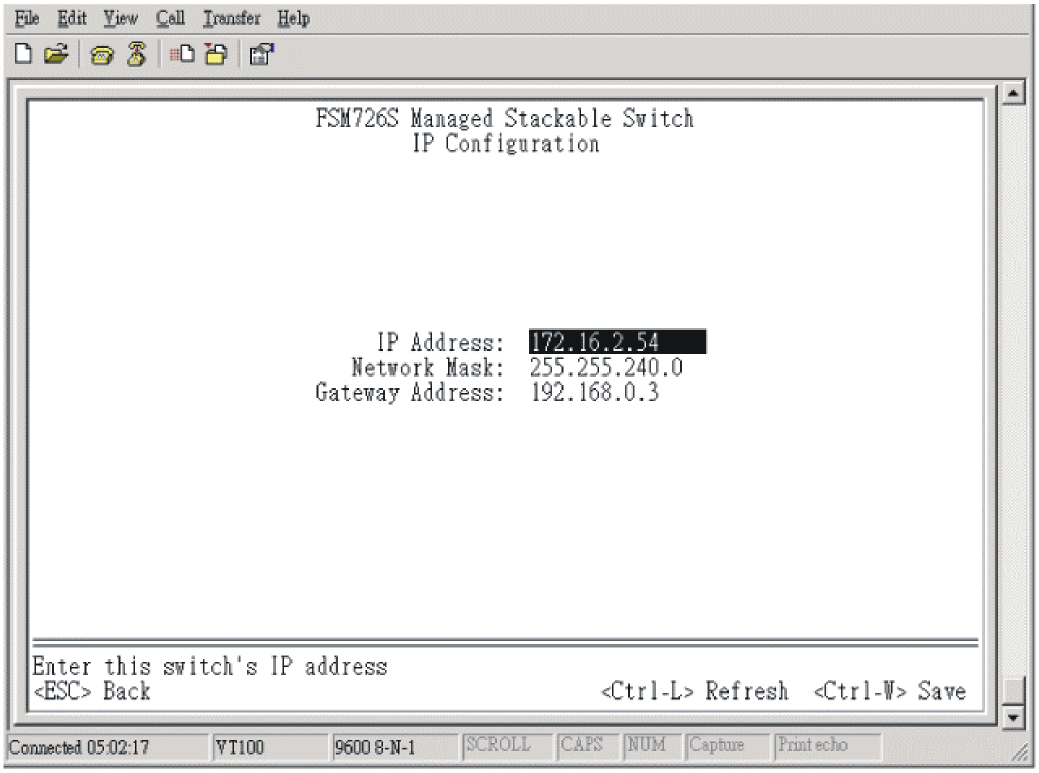
19. On the Main Menu page, hit the ‘C’ key to select the Set Up page



```
FSM726S Managed Stackable Switch
             Set-up

      a. Port Configuration
      b. IP Configuration

Hit <Enter> to configure Port Parameters
<ESC> Back                    <Ctrl-L> Refresh  <Ctrl-W> Save
```

Figure 4-6 Set-Up

20. On the Set Up page, hit the 'B' key to select the IP Configuration page.



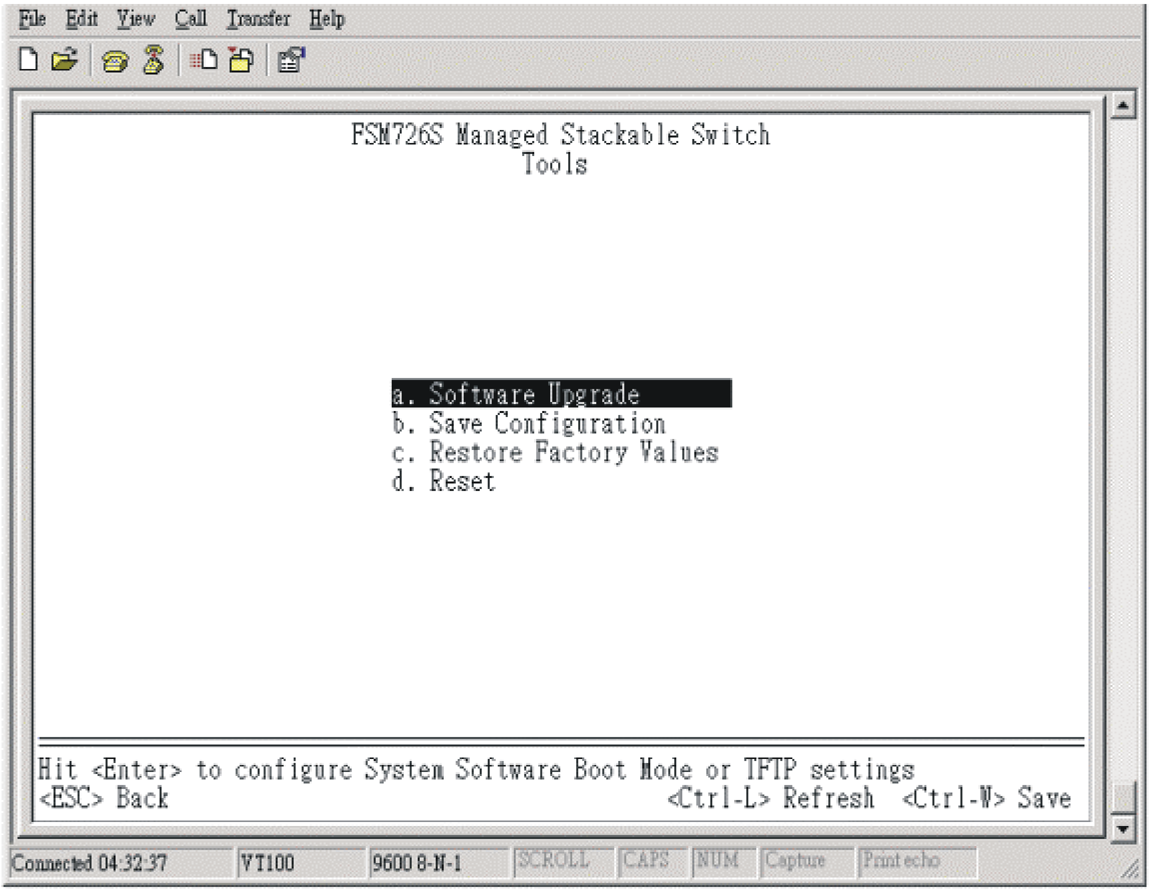
```
FSM726S Managed Stackable Switch
        IP Configuration

     IP Address:  172.16.2.54
   Network Mask:  255.255.240.0
Gateway Address:  192.168.0.3

Enter this switch's IP address
<ESC> Back                    <Ctrl-L> Refresh  <Ctrl-W> Save
```

Figure 4-7 IP Configuration

21. On the IP Configuration page, type in the desired IP Address for this switch, followed by the ‘Enter’ key.

Note: this switch is not DHCP client capable. You must assign a static IP address to the master switch.

22. Now type in the desired Network Mask, followed by the ‘Enter’ key.
23. Now type in the desired Default Gateway, followed by the ‘Enter’ key.
24. Use Ctrl-W to save these new settings. Hit the ‘Y’ key or ‘Enter’ to confirm saving the new settings to NVRAM.
25. Now hit the ‘ESC’ key twice to return to the Main Menu.
26. On the Main Menu page, hit the ‘D’ key to select the Tools page.



```
FSM726S Managed Stackable Switch
             Tools

a. Software Upgrade
b. Save Configuration
c. Restore Factory Values
d. Reset

Hit <Enter> to configure System Software Boot Mode or TFTP settings
<ESC> Back                            <Ctrl-L> Refresh  <Ctrl-W> Save
```

Figure 4-8: Tools page

27. On the Tools page, hit the ‘D’ key to Reset the switch. Hit the ‘Y’ key or ‘Enter’ to confirm resetting the switch.

The switch will now reset, loading the new IP address. At this point you can use your web browser to manage your switch through the network. After you have connected your computer to the switch via one of the network ports, simply launch your web browser and type the IP address in the Address Bar to use the Graphical User Interface (GUI) for configuration, observation, and management of your switch.

Step 8: Connecting Devices to the Switch

The following procedure describes how to connect devices to the switch’s RJ-45 ports. Your NETGEAR Model FSM726S Managed Stackable Switch contains Auto Uplink™ technology, which allows you to attach devices using either straight-through or crossover cables.

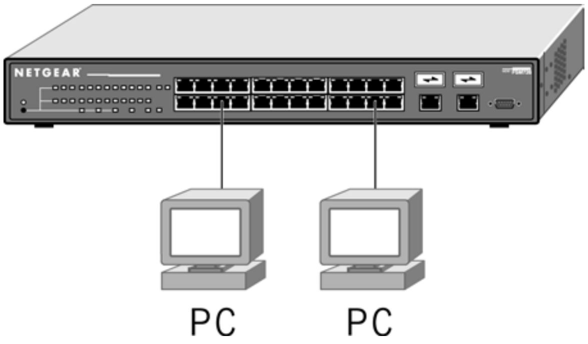


Figure 4-9. Connecting Devices to the Switch

28. Connect each device to an RJ-45 network port on the switch’s front panel (see Figure 4-9). Use Category 5 (Cat5) unshielded twisted-pair (UTP) cable terminated with an RJ-45 connector to make these connections.

Note: Ethernet specifications limit the cable length between the switch and the attached device to 100 m (328 ft).

Adding or Removing Switches to the stack

For the master unit to properly manage the stack, we recommend the following steps when adding or removing a switch from the stack

1. Power down all switches in the stack.

Note: Do not add or remove stacking cables while the switch is powered up.

2. Remove/Add the necessary switches

Note: the **Stack In** port on the master unit is always empty.

3. Power up the slave units in the stack.

4. Power up the master unit

CHAPTER 5: SWITCH MANAGEMENT OVERVIEW

This chapter gives an overview of switch management, including the methods you can use to manage your NETGEAR Model FSM726S Managed Stackable Switch. Topics include:

Management Access Overview

SNMP Access

Protocols

Software Upgrade Procedure

Management Access Overview

Your NETGEAR Model FSM726S Managed Stackable Switch gives you the flexibility to access and manage the switch using any or all of the following methods:

An administration console

Web browser interface

External SNMP-based network-management application

The administration console and Web browser interface support are embedded in the switch's firmware and available for immediate use. Each of these management methods has advantages. Table 5-1 compares the three management methods.

Table 5-1. Comparing Switch Management Methods

Management Method	Advantages	Disadvantages
Administration console	■ Out-of-band access via direct cable connection means network bottlenecks, crashes, and downtime do not slow or prevent access ■ No IP address or subnet needed ■ Menu-based ■ HyperTerminal access to full functionality (HyperTerminal are built into Microsoft Windows 95/98/NT/2000 operating systems) ■ Secure – MAKE SURE THE AREA WHERE THE SWITCH IS INSTALLED IS A SECURE AREA.	■ Must be near switch or use dial-up connection ■ Not convenient for remote users ■ Not graphical
Web browser	■ Can be accessed from any location via the switch's IP address ■ Ideal for configuring the switch remotely ■ Compatible with Internet Explorer and Netscape Navigator Web browsers ■ Familiar browser interface ■ Graphical data available ■ Most visually appealing	■ Security can be compromised (hackers need only know IP address and subnet mask) ■ May encounter lag times on poor connections ■ Displaying graphical objects over a browser interface may slow navigation
SNMP Agent	■ Communicates with switch functions at the Management Information Base (MIB) level ■ Based on open standards	■ Requires SNMP manager software ■ Least visually appealing of all three methods ■ Limited amount of information available ■ Some settings require calculations ■ Security can be compromised (hackers need only know the community name)

For a more detailed discussion of the Administration Console, see chapter 6. For a more detailed discussion of the Web Browser Interface, see chapter 7.

SNMP Access

With this access method, you can use an external Simple Network Management Protocol (SNMP) -based application to manage your NETGEAR Model FSM726S Managed Stackable Switch. Figure 5-1 shows an example of this management method.

This management method requires the SNMP agent on the switch and the SNMP Network Management Station to use the same community string. This management method, in fact, uses two community strings: the GET community string and the SET community string. If the SNMP Network management Station only knows the SET community string, it can read from and write to the MIBs. However, if it only knows the GETcommunity string, it can only read MIBs. The default GET community string for the switch is ‘public’.

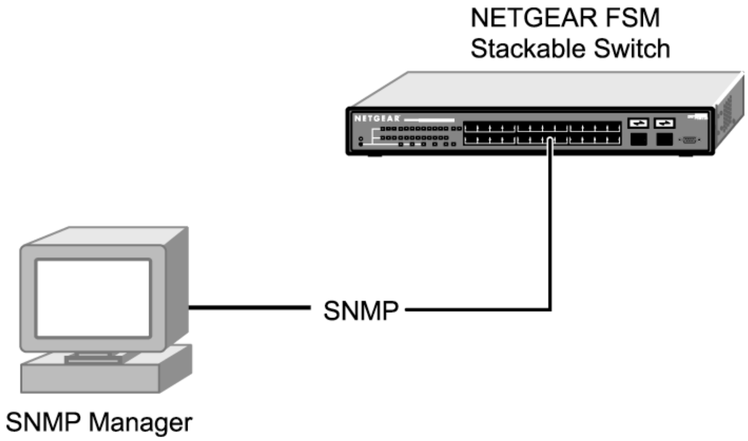


Figure 5-1. SNMP-Based Management Method

Protocols

Your NETGEAR Model FSM726S Managed Stackable Switch supports the following protocols:

Virtual terminal protocols, such as Telnet

SNMP

Virtual Terminal Protocols
A virtual terminal protocol is a software program, such as Telnet, that allows you to establish a management session from a Macintosh, a PC, or a UNIX workstation. Because Telnet runs over TCP/IP, you must have at least one IP address configured on the NETGEAR Model FSM726S Managed Stackable Switch before you can establish access to it with a virtual terminal protocol.

Terminal emulation differs from a virtual terminal protocol in that you must connect a terminal or PC directly to the console port. Figure 5-2 shows a UNIX workstation connected to the system through a virtual terminal protocol (Telnet), and a terminal connecting directly to the console port through a null-modem cable.

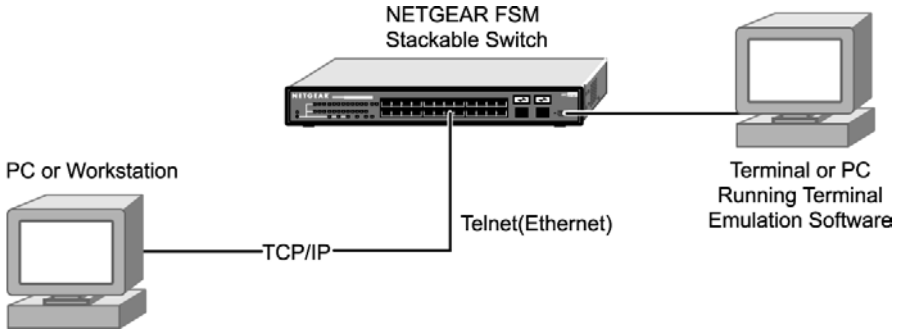


Figure 5-2. Administration Console Access

SNMP Protocol
SNMP is the standard management protocol for multi-vendor IP networks. SNMP supports transaction-based queries that allow the protocol to format messages and to transmit information between reporting devices and data-collection programs. SNMP runs on top of the User Datagram Protocol (UDP), offering a connectionless-mode service.

Software Upgrade Procedure

The application software is field upgradeable. The upgrade procedure and the required equipment is described in the following section.

Note that once the system is up, it is controlled by an executing application image residing in non-volatile memory. No software upgrade is possible during this mode. The upgrade can only be done when the system is resetting. To initiate this sequence, the user must set the ‘Next Boot From’ configuration parameter to ‘Boot from Net’ during normal operation, and then perform a ‘reset’. When the ‘Boot from Net’ option is set, the switch will start using an image residing on a TFTP server on the network. Be sure that the TFTP server residing on the network is accessible by the switch. Once completed, the software version should be verified in the System page.

Note: It is highly recommended, though not necessary, to use a RS-232 serial port connection to the switch during the software upgrading procedure. When using a Telnet Session or web interface alone, your connection to the switch will not be available until the switch has entered forwarding mode. This takes approximately three minutes.

The upgrade procedure is as follow:

1. Go to Main Menu>Tools>Software Upgrade (in the Web or Console Interface).
2. Select 'Boot from Net' option.
3. Verify information such as the IP address for the TFTP Server, Gateway IP address, and the file name and its path of the new image.
4. Save the setting in non-volatile memory. In the Browser interface, use the 'Apply' button, and the Tools> Save Configuration screen. In the console interface, use Ctrl-W and confirm the change to NVRAM.
5. Restart the system via the Tools>Reset command
6. Bootstrap will retrieve the new image then pass control to it.
7. The system executes the new software image.

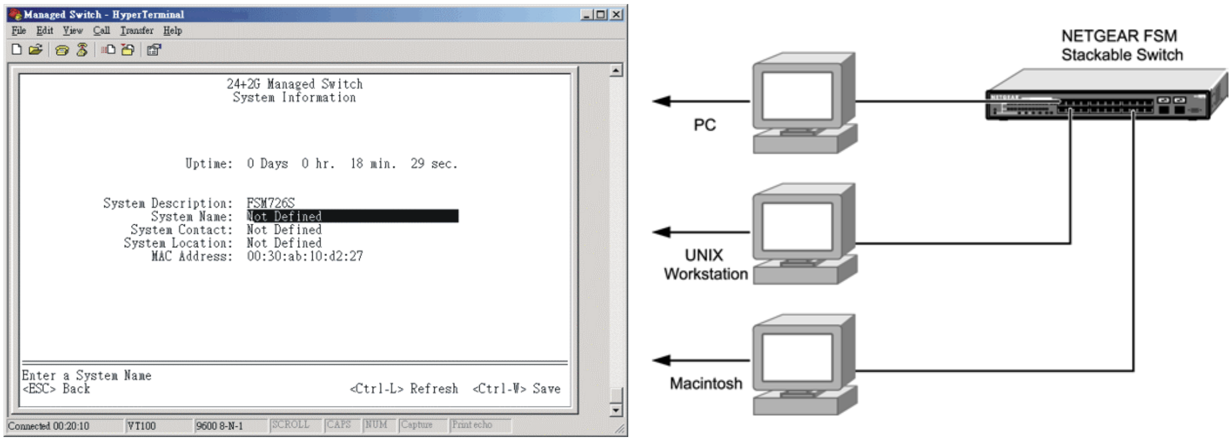
Note: the previous image in non-volatile memory will not be replaced by the new image using this option. The image in non-volatile memory will only be over-written if 'Boot from Net and Save' option is selected.

8. Test your switch to make sure the new image is working correctly. If you decide to keep the new image, go to Software Download again. Select 'Boot from Net & Save' option.
9. Save the setting in non-volatile memory. In the Browser interface, use the 'Apply' button, and the Tools> Save Configuration screen. In the console interface, use Ctrl-W and confirm the change to NVRAM.
10. Restart the system via the Tools>Reset command
11. The new image should over-write the old image in non-volatile memory. Verify it by going to the Software Download screen and checking the Software Release information.

Note: IP address, Network Mask, and Default Gateway are not affected by upgrading the software. The settings will still be in non-volatile memory.

CHAPTER 6: ADMINISTRATION CONSOLE ACCESS

The administration console is an internal, character-oriented, VT-100/ANSI menu-driven user interface for performing management activities. Using this method, you can view the administration console from a terminal, PC, Apple Macintosh, or UNIX workstation connected to the switch's console port. Figure 6-1 shows an example of this management method.



```
                       24+2G Managed Switch
                        System Information



               Uptime:  0 Days  0 hr.  18 min.  29 sec.


   System Description:  FSM726S
          System Name:  Not Defined
       System Contact:  Not Defined
      System Location:  Not Defined
          MAC Address:  00:30:ab:10:d2:27







Enter a System Name
<ESC> Back                              <Ctrl-L> Refresh  <Ctrl-W> Save
```

Figure 6-1. Administration Console Management Method

Direct Access

Direct access to the switch console is achieved by connecting the switch's console port to a VT-100 or compatible terminal or to a PC, Apple Macintosh, or UNIX workstation equipped with a terminal-emulation program. This connection is made using the null-modem cable supplied with the switch.

The following list provides examples of terminal-emulation programs:

HyperTerminal (which is built into the Microsoft Windows operating systems)

ZTerm (Apple Macintosh)

TIP (UNIX workstation)

The terminal-emulation program should use the following settings:

Baud rate: 9,600 bps

Data bits: 8

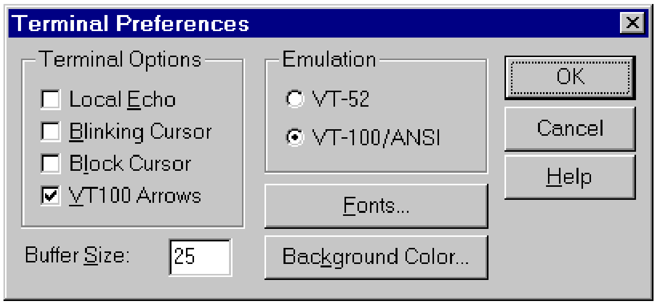
Parity: none

Stop bit: 1

Flow control: none

The direct access management method is required when you configure the switch for the first time. Thereafter, we recommend you use the Web management access method (described in chapter 7) to manage the switch.

The console, using VT100 terminal emulation, can be accessed from the RS-232 serial port or a telnet connection. The switch offers password protection for this interface. All of the following examples of the Console's User Interface show a screen capture from a telnet session.



Terminal Preferences

Terminal Options

□ Local Echo

□ Blinking Cursor

□ Block Cursor

☑ VT100 Arrows

Emulation

○ VT-52

● VT-100/ANSI

Buffer Size: 25

When attached to the User Interface via a Telnet Session, the following must be set in order to use the arrow keys: Under the terminal pull down menu choose Properties and make sure the VT100 Arrows option is turned on.

User Interface

The switch offers a menu-driven interface.

Characteristics

There are several characteristics to the User Interface pages that are necessary to know before proceeding to use it. The TAB key or the arrow keys may be used to move within menus and sub-screens. At the bottom of every screen are some key commands available to the user for that particular screen, as well as some helpful information.

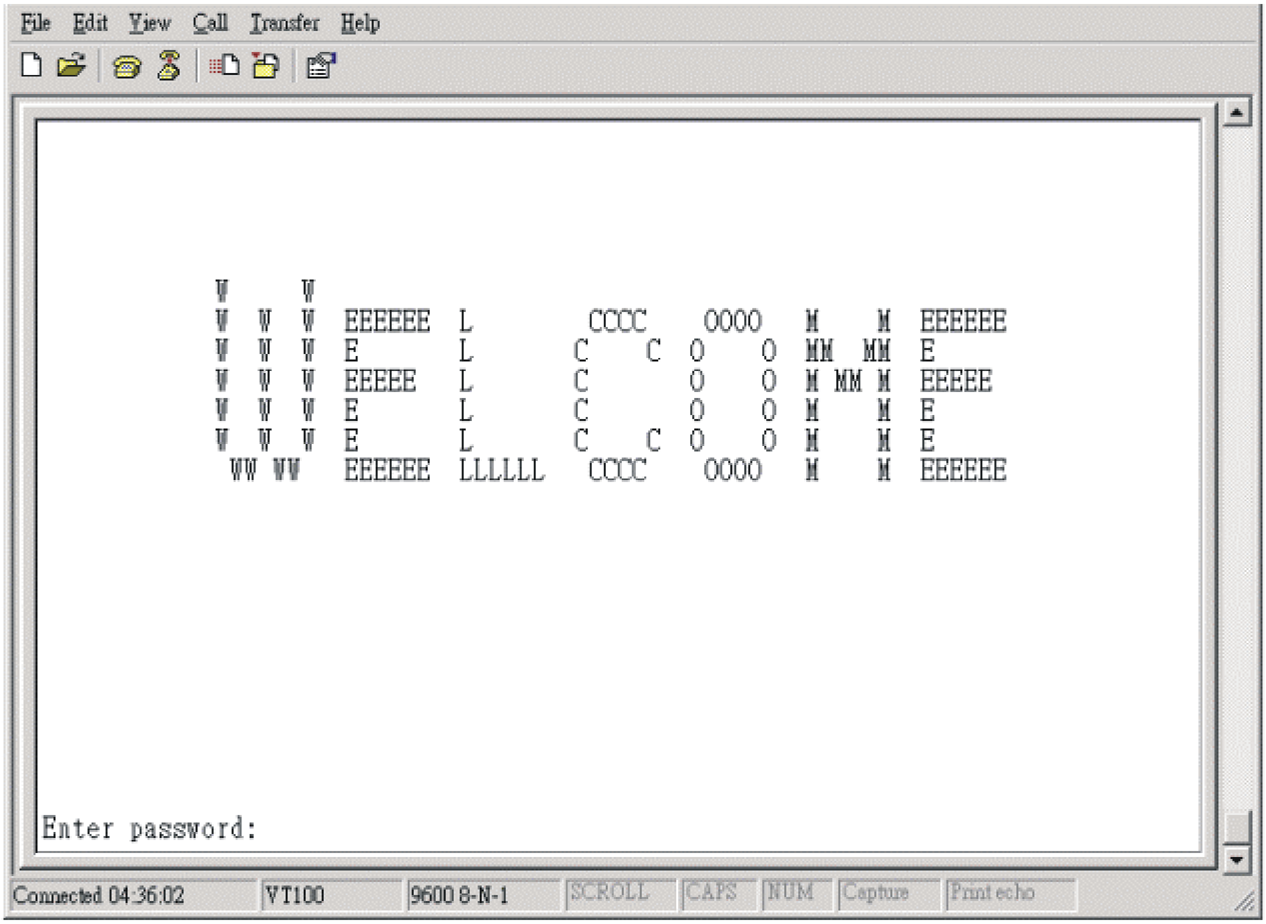
The common keystrokes and their definitions and intricacies are listed below:

ESC	Return to the previous menu or screen, or abort editing
Tab	Select field
Ctrl-L	Refresh the screen
Ctrl-D	Log off (password enabled)
Ctrl-M	Move to field (Switch Statistics and Port Configuration menus only)
Ctrl-W	Saves current configuration to Non-Volatile RAM (NVRAM)
Spacebar	Toggles between possible settings for a field
Enter	Select a menu item, edit a field, or accept a value after editing a field
Ctrl-X	Delete a table entry

The initial screen depends on if password protection has been enabled. If it has, it is the welcome screen, seen below in Figure 6-2. If there is no password set on the system, the Main Menu will be displayed and access is granted immediately. By default, password protection is disabled. If enabled, the default password is ‘1234’.

To enable password protection:

- Choose Security from the Main Menu
- Toggle Password Protection to Enabled
- Enter and verify new password
- Save with Ctrl-W



```
W     W
W  W  W  EEEEEE  L        CCCC    OOOO   M    M  EEEEEE
W  W  W  E       L       C    C  O    O  MM  MM  E
W  W  W  EEEEE   L       C       O    O  M MM M  EEEEE
W  W  W  E       L       C       O    O  M    M  E
W  W  W  E       L       C    C  O    O  M    M  E
 WW WW   EEEEEE  LLLLLL   CCCC    OOOO   M    M  EEEEEE




Enter password:
```

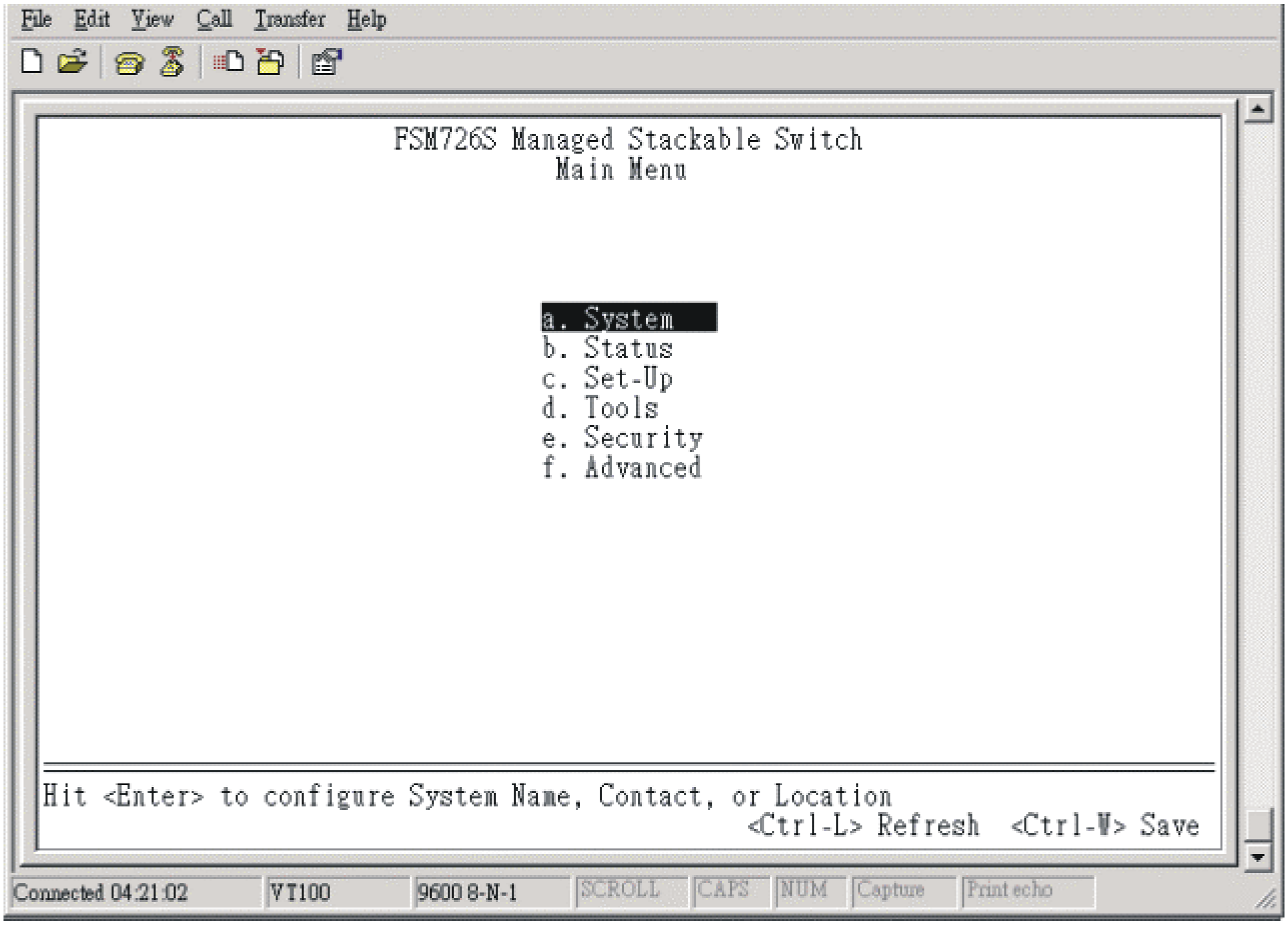
Figure 6-2 Initial Welcome screen of User Interface (Password enabled)

Main Menu

The main menu displays all the sub-menus that are available. Striking ‘Enter’ when an option is highlighted will confirm the choice of the specified sub-menu. The ‘hotkey’ or letter in front of each menu option can also be typed to directly choose that option. As shown in Figure 6-3, there are six menu items to choose from:

- System
- Status
- Set-Up
- Tools
- Security
- Advanced

To logout of the user interface, hit Ctrl-D at anytime during your telnet session. You will be brought back to the login screen (password enabled) or Main Menu (password disabled).



```
                FSM726S Managed Stackable Switch
                           Main Menu



                          a. System
                          b. Status
                          c. Set-Up
                          d. Tools
                          e. Security
                          f. Advanced



Hit <Enter> to configure System Name, Contact, or Location
                              <Ctrl-L> Refresh  <Ctrl-W> Save
```

Figure 6-3: Main Menu

Main Menu> System

This screen displays the following:

System uptime

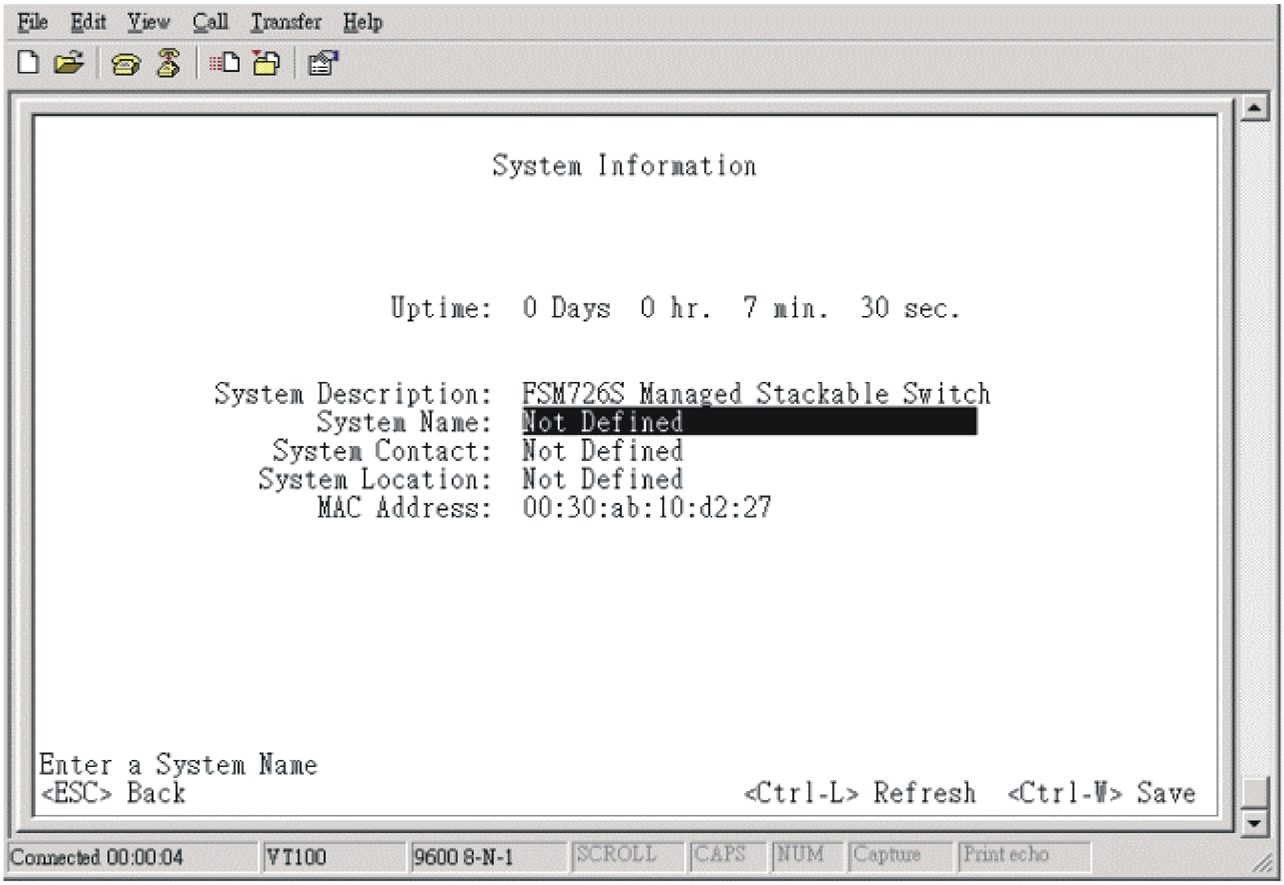
System Description

System Name- user definable

System Contact-user definable

System Location-user definable

MAC Address



```
                          System Information



                    Uptime:  0 Days  0 hr.  7 min.  30 sec.


        System Description:  FSM726S Managed Stackable Switch
               System Name:  Not Defined
            System Contact:  Not Defined
           System Location:  Not Defined
               MAC Address:  00:30:ab:10:d2:27






Enter a System Name
<ESC> Back                               <Ctrl-L> Refresh  <Ctrl-W> Save
```

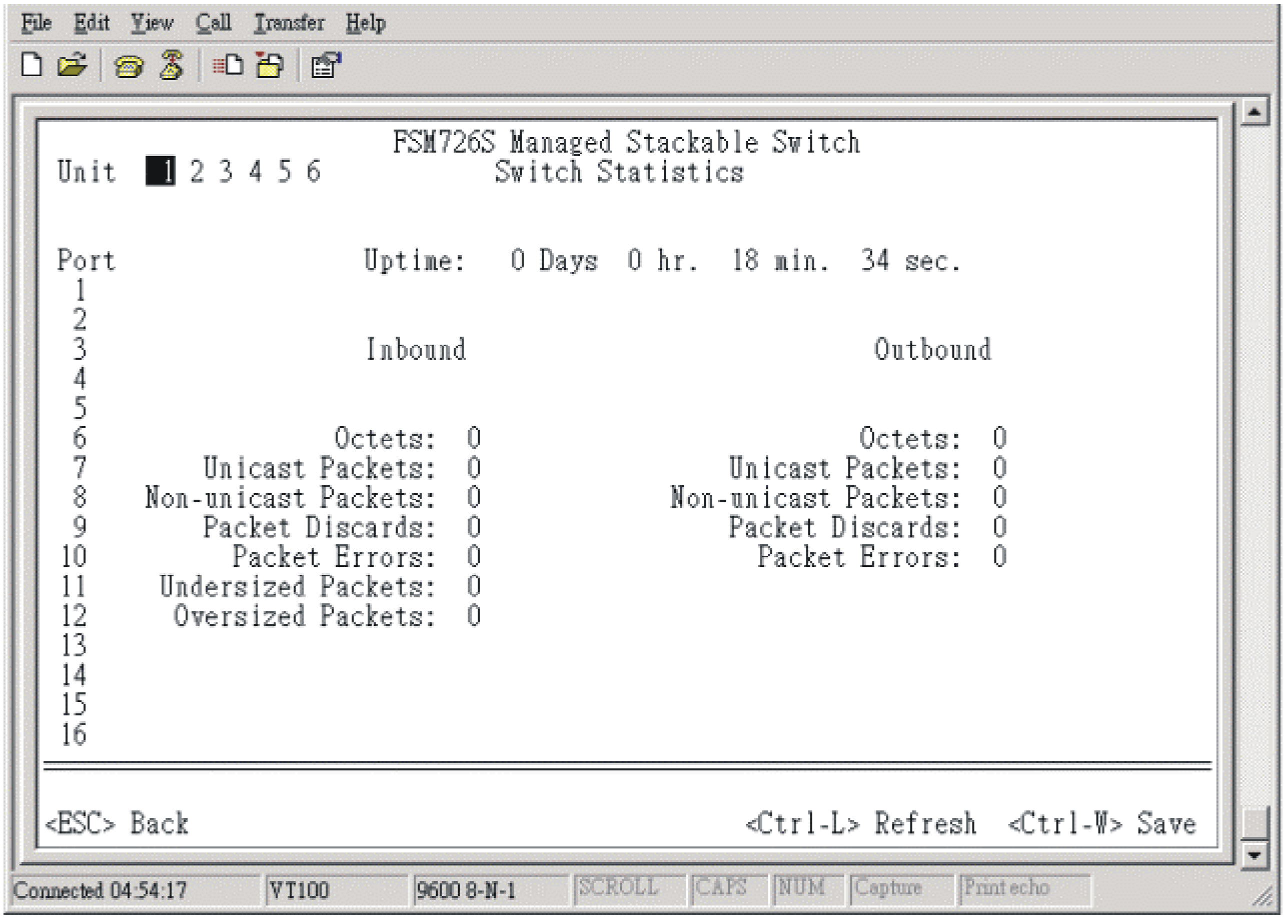
Figure 6-4: System Information

Main Menu> Status

There are two sub-menus at Status menu, the Switch Statistics and MAC Address Table.

Main Menu> Status >Statistics

There are two sections in this screen. The Unit number at the top indicates the switch in the stack, and left-side Port-ID field allows you to choose a port to be observed. To get to the left side, use Ctrl-M to move to that field. The central portion of the screen displays the basic statistics associated with the port, which is highlighted at the Port-ID field.

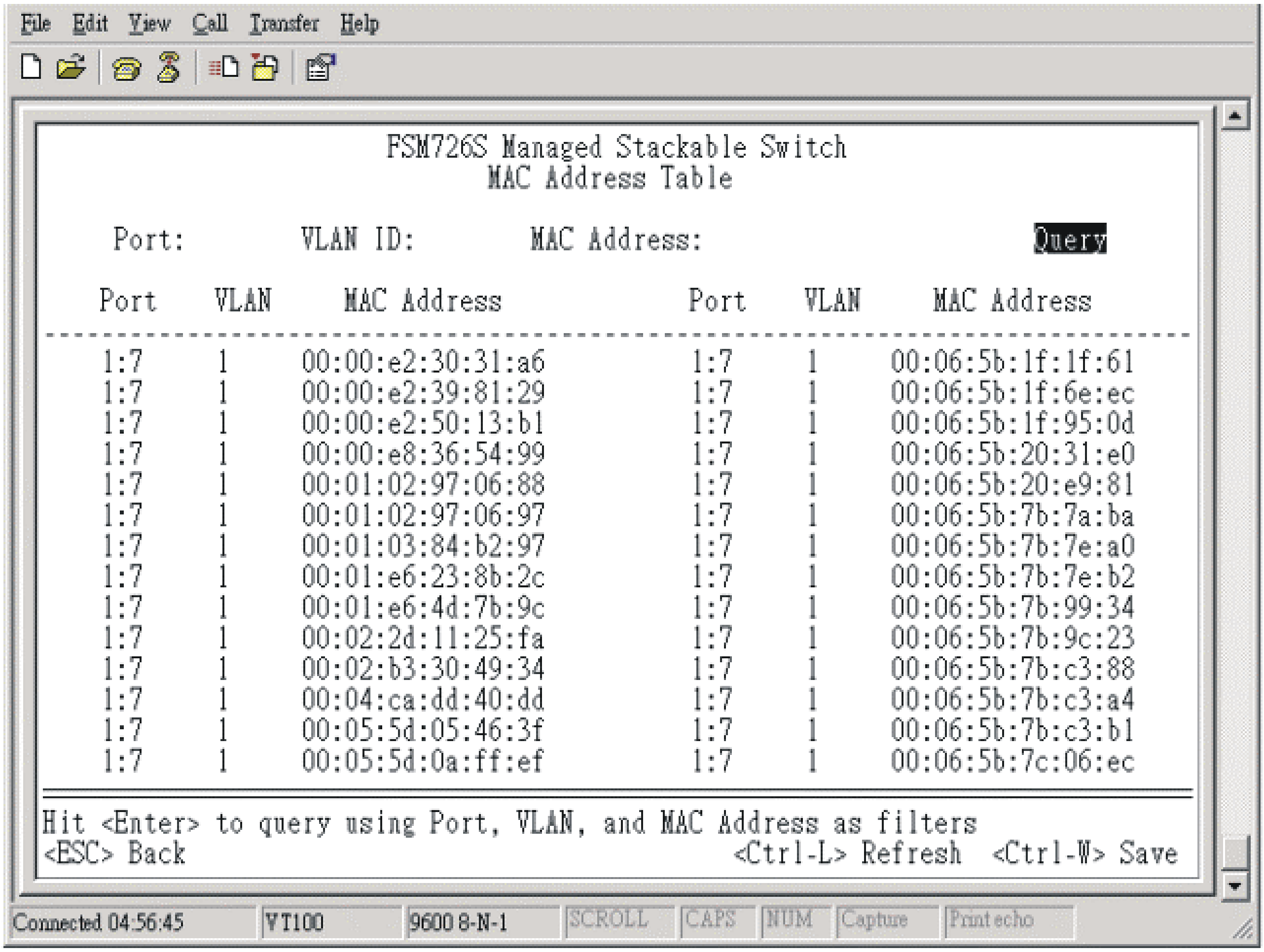


```
                           FSM726S Managed Stackable Switch
Unit  1 2 3 4 5 6                  Switch Statistics


Port                  Uptime:   0 Days  0 hr.  18 min.  34 sec.
 1
 2
 3                    Inbound                            Outbound
 4
 5
 6                 Octets:  0                         Octets:  0
 7        Unicast Packets:  0                Unicast Packets:  0
 8    Non-unicast Packets:  0            Non-unicast Packets:  0
 9        Packet Discards:  0                Packet Discards:  0
10          Packet Errors:  0                  Packet Errors:  0
11     Undersized Packets:  0
12      Oversized Packets:  0
13
14
15
16

<ESC> Back                                <Ctrl-L> Refresh  <Ctrl-W> Save
```

Figure 6-5: Statistics

Main Menu> Status > MAC Address Table (Dynamic Addresses)

The MAC Address lookup table allows you to view the dynamic MAC addresses that are currently in the address database. When addresses are in the database, the packets intended for those addresses are forwarded directly to those ports. You can filter out addresses in the table by port, VLAN, and/or MAC address by entering a value in those fields, and selecting ‘Query’.



```
                         FSM726S Managed Stackable Switch
                                MAC Address Table

      Port:        VLAN ID:        MAC Address:                      Query

     Port     VLAN      MAC Address                Port     VLAN      MAC Address
 -------------------------------------------------------------------------------
     1:7      1       00:00:e2:30:31:a6            1:7      1       00:06:5b:1f:1f:61
     1:7      1       00:00:e2:39:81:29            1:7      1       00:06:5b:1f:6e:ec
     1:7      1       00:00:e2:50:13:b1            1:7      1       00:06:5b:1f:95:0d
     1:7      1       00:00:e8:36:54:99            1:7      1       00:06:5b:20:31:e0
     1:7      1       00:01:02:97:06:88            1:7      1       00:06:5b:20:e9:81
     1:7      1       00:01:02:97:06:97            1:7      1       00:06:5b:7b:7a:ba
     1:7      1       00:01:03:84:b2:97            1:7      1       00:06:5b:7b:7e:a0
     1:7      1       00:01:e6:23:8b:2c            1:7      1       00:06:5b:7b:7e:b2
     1:7      1       00:01:e6:4d:7b:9c            1:7      1       00:06:5b:7b:99:34
     1:7      1       00:02:2d:11:25:fa            1:7      1       00:06:5b:7b:9c:23
     1:7      1       00:02:b3:30:49:34            1:7      1       00:06:5b:7b:c3:88
     1:7      1       00:04:ca:dd:40:dd            1:7      1       00:06:5b:7b:c3:a4
     1:7      1       00:05:5d:05:46:3f            1:7      1       00:06:5b:7b:c3:b1
     1:7      1       00:05:5d:0a:ff:ef            1:7      1       00:06:5b:7c:06:ec
 ===============================================================================
 Hit <Enter> to query using Port, VLAN, and MAC Address as filters
 <ESC> Back                                          <Ctrl-L> Refresh  <Ctrl-W> Save
```

Figure 6-6: Address Manager: MAC Address Table

Main Menu> Set-Up

There are two sub-menus at Set-Up menu, Port Configuration and IP Configuration.

Main Menu> Set-Up> Port Configuration

On this page, you can set up the port characteristics related to link operations (see Figure 6-7). All of the parameters on this page are toggle settings. To change, or toggle, between options, hit Ctrl-M to move the curser to the ports field and simply strike the space bar when the appropriate option is highlighted. To modify ports 17 to 26, you must tab through ports 1 to 16. The comments field is available for you to enter a description of the port.

Admin field
Allows you to Enable or Disable the port.

State
The State field displays the Spanning Tree State of the port (Blocking, Listening, Learning, Forwarding, or Disabled). You can only observe the status of the ports; you cannot modify this field. The Spanning Tree Protocol controls this field.

Rate/Duplex field
Offers the choice of Full-duplex, Half-duplex, or Auto negotiation.
Enabling auto-negotiation on a port allows a port to sense the communication speed and negotiate the duplex mode (full duplex or half duplex) automatically. The ports will select the highest possible throughput. The port can auto-negotiate with any port that is compliant with IEEE 802.3u. If the other port is not IEEE802.3u compliant, the port will default to half-duplex, 10 Mbps mode. Users can operate the communication speed and duplex mode manually.

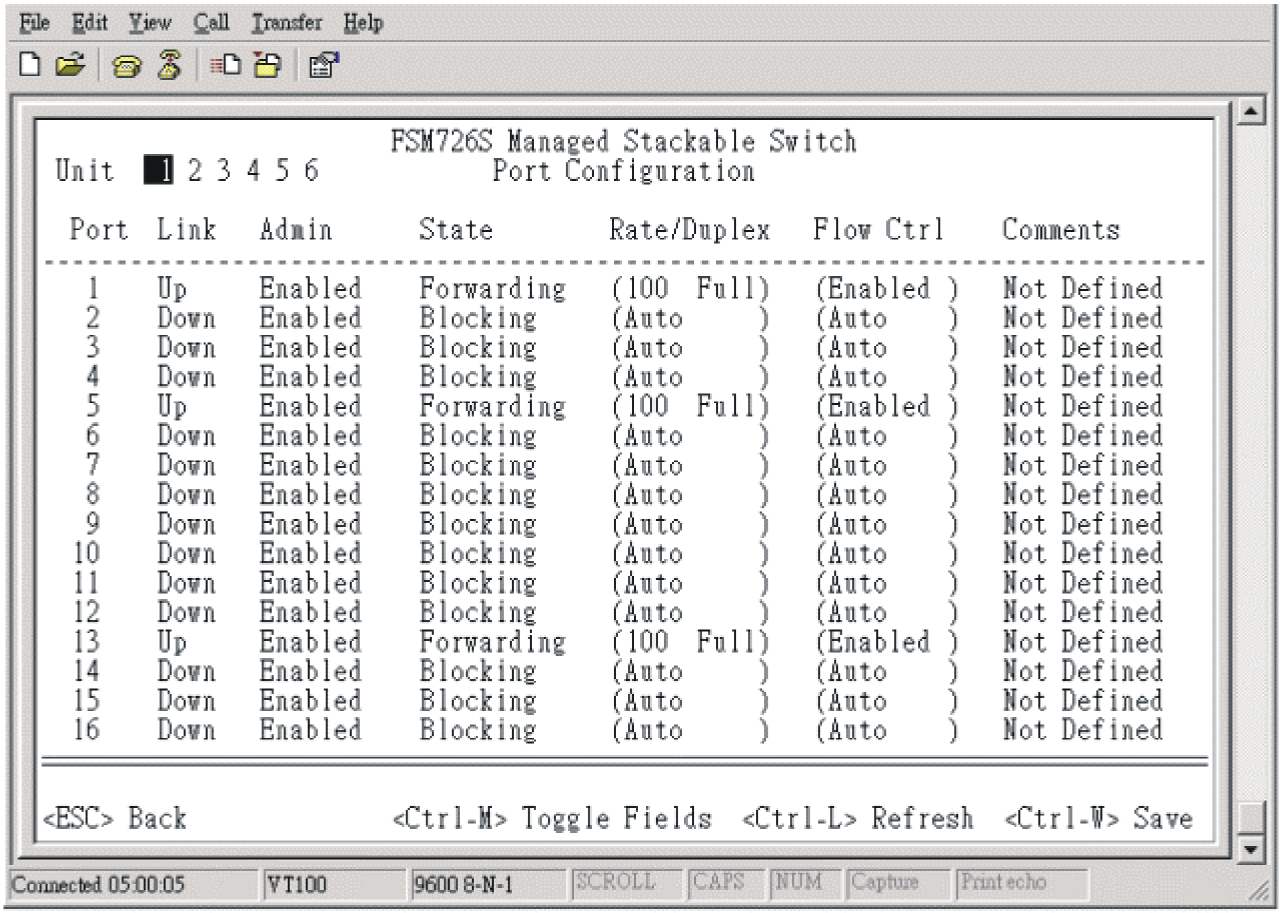
Flow Control
Allows you to enable or disable Flow Control.
Flow control is a protocol that prevents packets from being dropped by reducing the amount of traffic to a level that can be accommodated. If enabled on both ends of a connection, it will prevent the sender from sending data until the receiver can accept it. This switch complies with the IEEE802.3x flow control standard.

Comments
Allows you to name the port or make notes.

Gigabit Ports
For the two gigabit ports on each switch in the stack, the port type may be chosen. The default is that the port uses the RJ-45 interface. If so chosen, the user may use a GBIC interface. If so, the user must switch the port type from ‘GT’ to ‘GB’. This can be done by hitting the space bar on the two letters next to the port number.

Note: enabling the GBIC connector for a Gigabit Ethernet port disables the built-in 1000BASE-T port.

Note: GBIC ports do not support Auto Negotitation. You must manually configure the GBIC port. The default values are 1000 Mbps, full duplex.



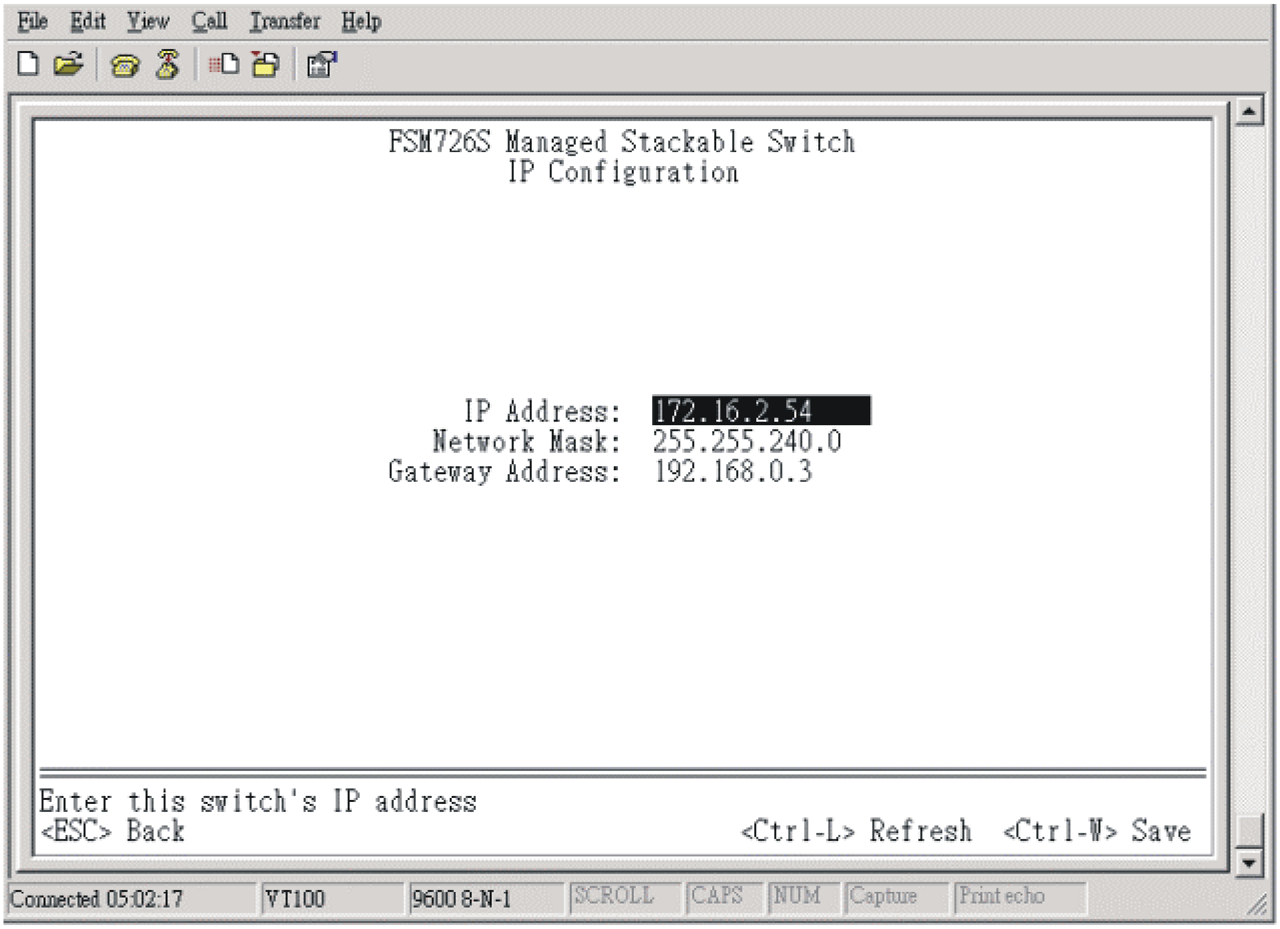
```
                         FSM726S Managed Stackable Switch
Unit  1 2 3 4 5 6               Port Configuration

 Port  Link  Admin     State       Rate/Duplex  Flow Ctrl    Comments
----------------------------------------------------------------------------
   1   Up    Enabled   Forwarding  (100  Full)  (Enabled )   Not Defined
   2   Down  Enabled   Blocking    (Auto     )  (Auto    )   Not Defined
   3   Down  Enabled   Blocking    (Auto     )  (Auto    )   Not Defined
   4   Down  Enabled   Blocking    (Auto     )  (Auto    )   Not Defined
   5   Up    Enabled   Forwarding  (100  Full)  (Enabled )   Not Defined
   6   Down  Enabled   Blocking    (Auto     )  (Auto    )   Not Defined
   7   Down  Enabled   Blocking    (Auto     )  (Auto    )   Not Defined
   8   Down  Enabled   Blocking    (Auto     )  (Auto    )   Not Defined
   9   Down  Enabled   Blocking    (Auto     )  (Auto    )   Not Defined
  10   Down  Enabled   Blocking    (Auto     )  (Auto    )   Not Defined
  11   Down  Enabled   Blocking    (Auto     )  (Auto    )   Not Defined
  12   Down  Enabled   Blocking    (Auto     )  (Auto    )   Not Defined
  13   Up    Enabled   Forwarding  (100  Full)  (Enabled )   Not Defined
  14   Down  Enabled   Blocking    (Auto     )  (Auto    )   Not Defined
  15   Down  Enabled   Blocking    (Auto     )  (Auto    )   Not Defined
  16   Down  Enabled   Blocking    (Auto     )  (Auto    )   Not Defined

<ESC> Back              <Ctrl-M> Toggle Fields  <Ctrl-L> Refresh  <Ctrl-W> Save
```

Figure 6-7: Port Configuration

Main Menu> Set-Up> IP Configuration

This menu manages the IP related information of the system.

- Enter a site-specific IP address, Gateway Address, and Network Mask (or subnet mask). Consult your network administrator for the information.
- Press Ctrl-W to save any changes to NVRAM.



```
                    FSM726S Managed Stackable Switch
                           IP Configuration



                      IP Address:  172.16.2.54
                    Network Mask:  255.255.240.0
                 Gateway Address:  192.168.0.3



Enter this switch's IP address
<ESC> Back                              <Ctrl-L> Refresh   <Ctrl-W> Save
```

Figure 6-8: Set-up Manager: IP Configuration

Main Menu> Tools

There are some system setup tools provided:

- Software Upgrade
- Save Configuration
- Restore Factory Values
- Reset

Main Menu> Tools> Software Upgrade

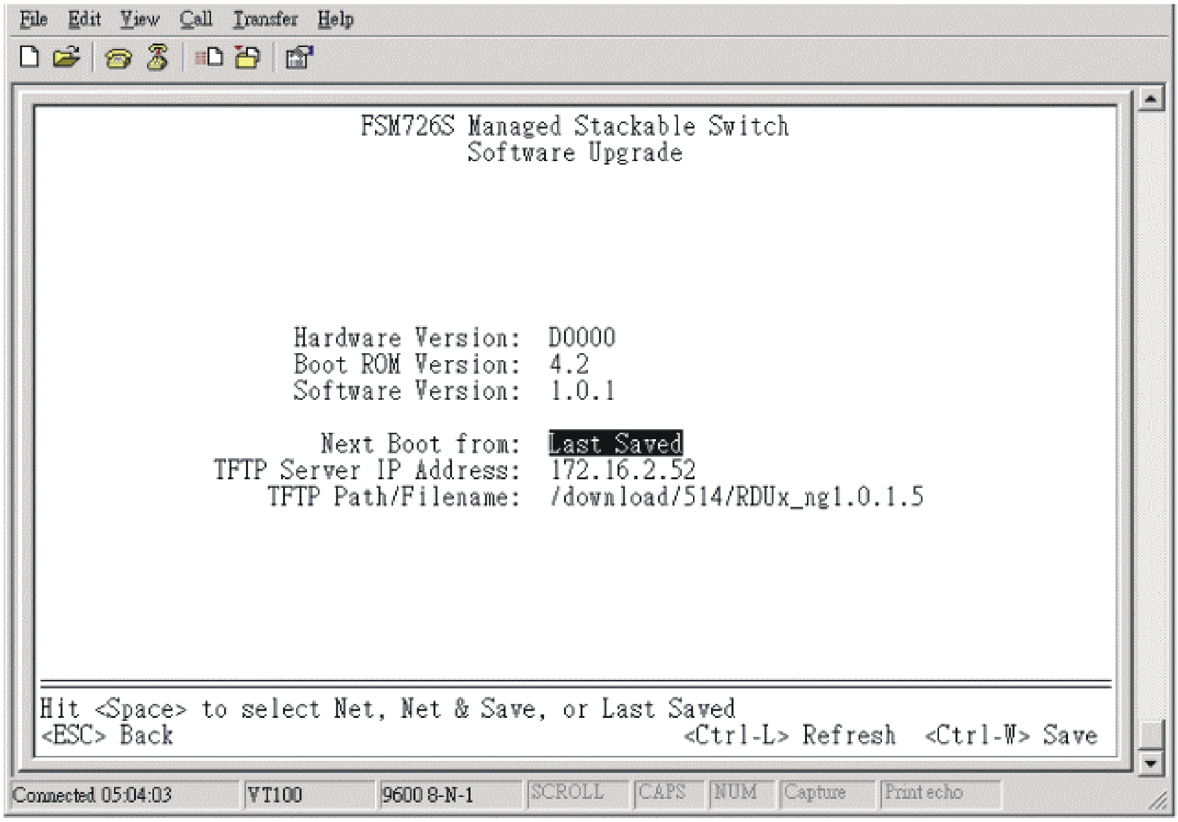
This screen allows you to select an image file and the location from where it can be downloaded using TFTP. There are three 'Boot from:' options: Net, Net & Save, and Last Saved. Please refer to Chapter 5 when updating software.

Net option:
This option allows you to try out a new image before upgrading. It requires a TFTP filename and a server IP address to retrieve the specified image from the given IP address.
The new image will not overwrite the one in non-volatile memory.

Net & save option
This option requires the same setup as the Net option, i.e. TFTP server and a new image. However, it copies the image to non-volatile memory directly and then the system boots from non-volatile memory

Warning: The previous image in non-volatile memory will be lost when the procedure completes.

Last Saved option
The system will boot from non-volatile memory. This option will automatically show up after the 'Net & save' option is selected and the unit is reset.



```
                    FSM726S Managed Stackable Switch
                            Software Upgrade



              Hardware Version:  D0000
              Boot ROM Version:  4.2
              Software Version:  1.0.1

                Next Boot from:  Last Saved
         TFTP Server IP Address:  172.16.2.52
             TFTP Path/Filename:  /download/514/RDUx_ng1.0.1.5

Hit <Space> to select Net, Net & Save, or Last Saved
<ESC> Back                                <Ctrl-L> Refresh  <Ctrl-W> Save
```

Figure 6-9: Software Update

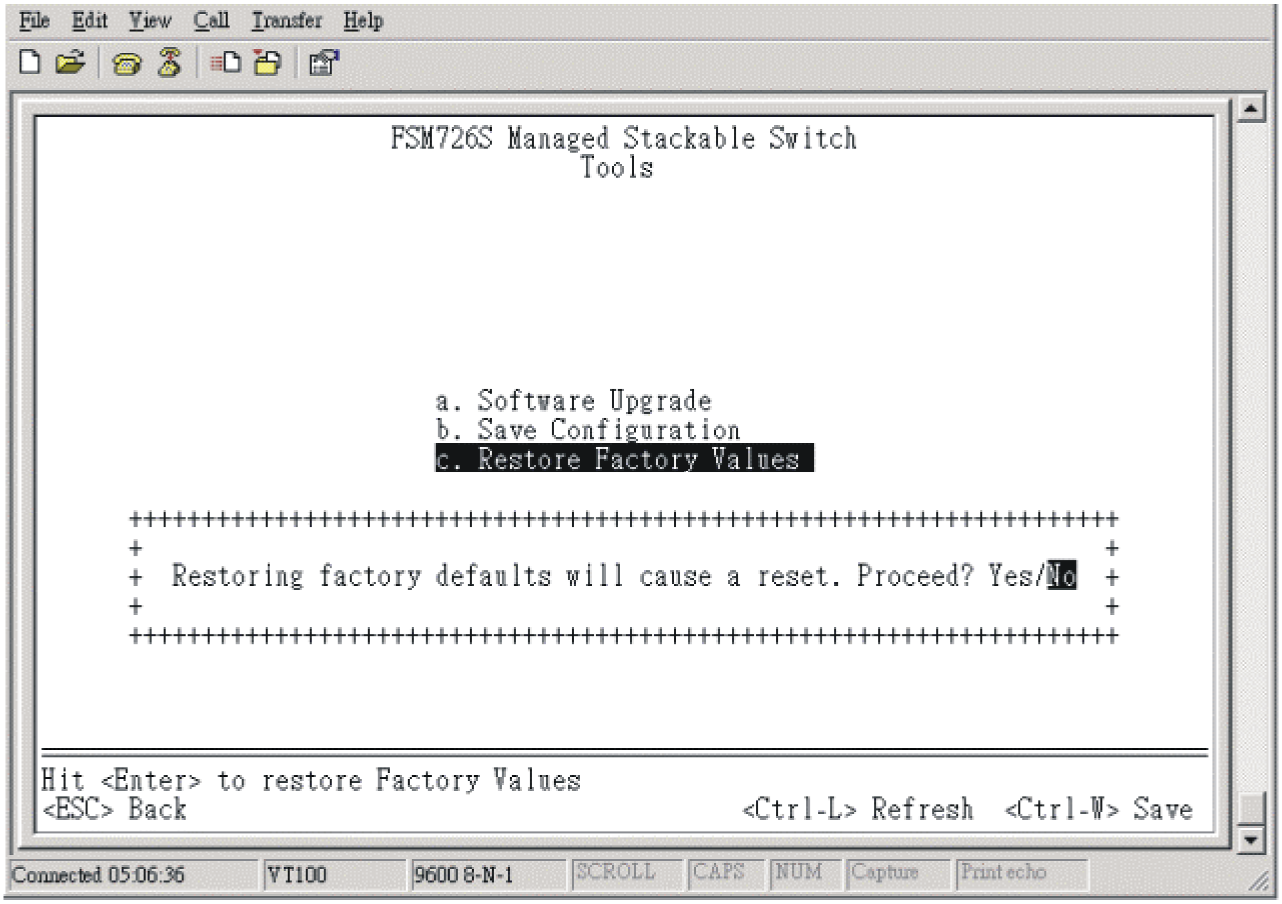
Main Menu> Tools> Save Configuration

After making any changes to the screens within the console interface, users must save the changed settings to NVRAM.

<u>Save Configuration to NVRAM</u>
Select Save Configuration and then use either 'Enter' or 'Y' to save the configuration to NVRAM.

<u>Restore Factory Values</u>
Select Restore Factory Values to reset the switch parameters to their original default settings. In order for changes to take effect, you must Reset the switch.

Note: network IP settings (i.e. IP address, Gateway Address, Network Mask) will not be affected by this command.

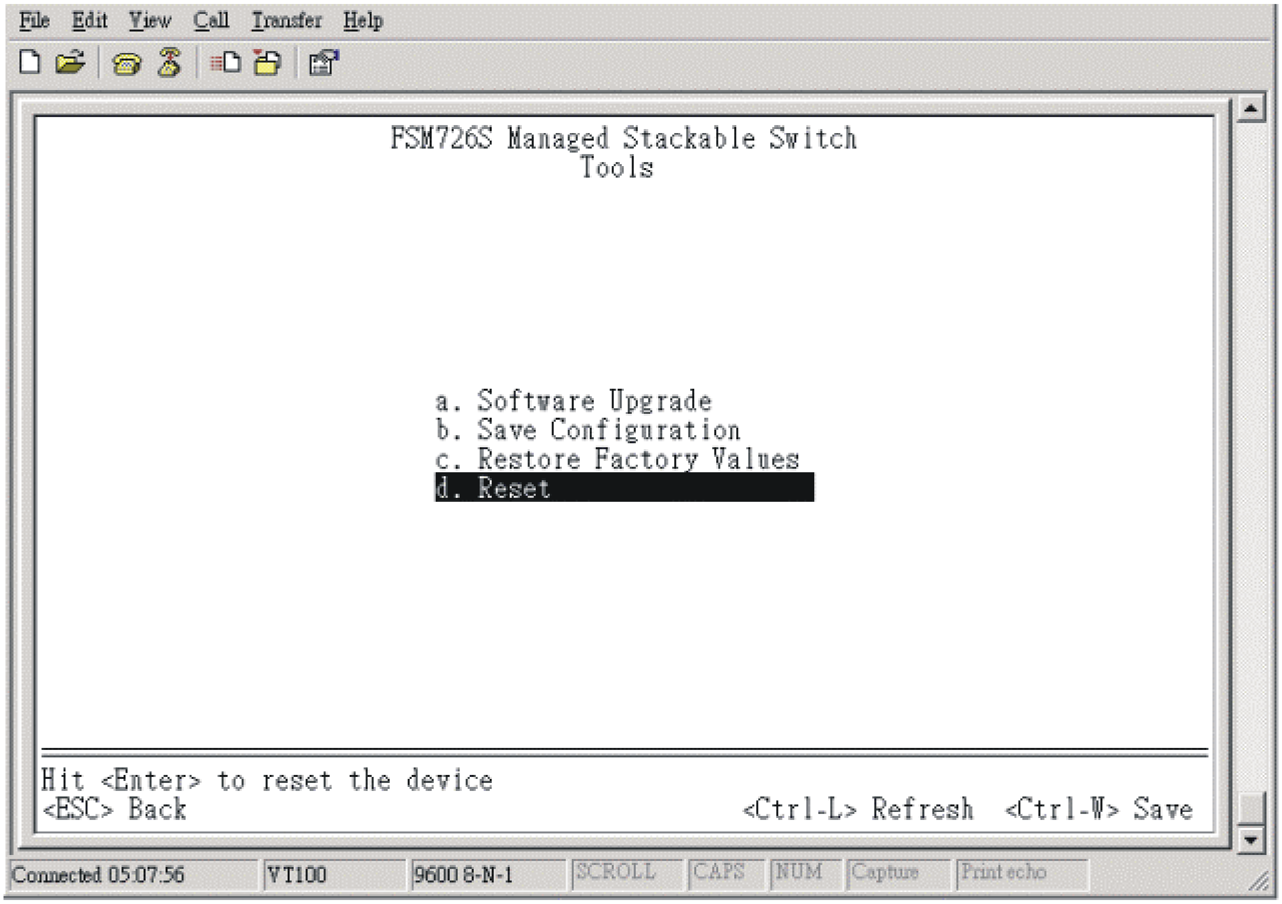


```
                        FSM726S Managed Stackable Switch
                                     Tools




                           a. Software Upgrade
                           b. Save Configuration
                           c. Restore Factory Values

      ++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
      +                                                                  +
      +  Restoring factory defaults will cause a reset. Proceed? Yes/No  +
      +                                                                  +
      ++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++



Hit <Enter> to restore Factory Values
<ESC> Back                                       <Ctrl-L> Refresh  <Ctrl-W> Save
```

Figure 6-10: Restore Factory Values

Main Menu> Tools> Reset

Reset Switch will restart the switch, the equivalent of turning the power off and on. Reset switch will clear the statistical counters to zero.



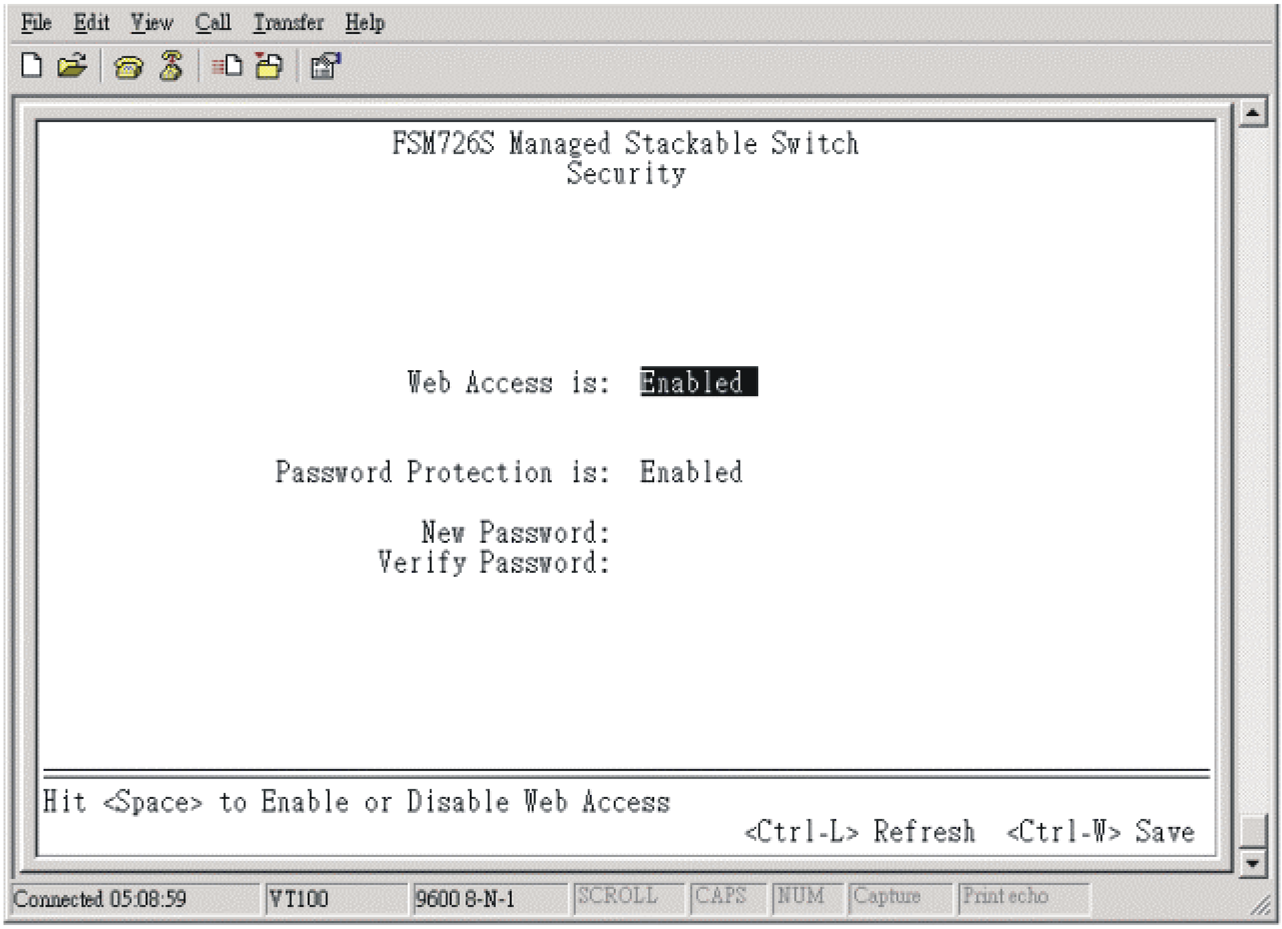
```
                    FSM726S Managed Stackable Switch
                                Tools




                    a. Software Upgrade
                    b. Save Configuration
                    c. Restore Factory Values
                    d. Reset





Hit <Enter> to reset the device
<ESC> Back                              <Ctrl-L> Refresh  <Ctrl-W> Save
```

Figure 6-11: Reset

Main Menu> Security

This screen allows the user to enable or disable the web interface and change the password for both the Console and Web sessions. To use password protection, you must enable Password Protection.

If you forget your password, contact NETGEAR technical support at 1-888-NETGEAR.



```
                    FSM726S Managed Stackable Switch
                               Security




                        Web Access is:  Enabled

               Password Protection is:  Enabled

                         New Password:
                      Verify Password:




Hit <Space> to Enable or Disable Web Access
                                      <Ctrl-L> Refresh  <Ctrl-W> Save
```

Figure 6-12: Security Admin

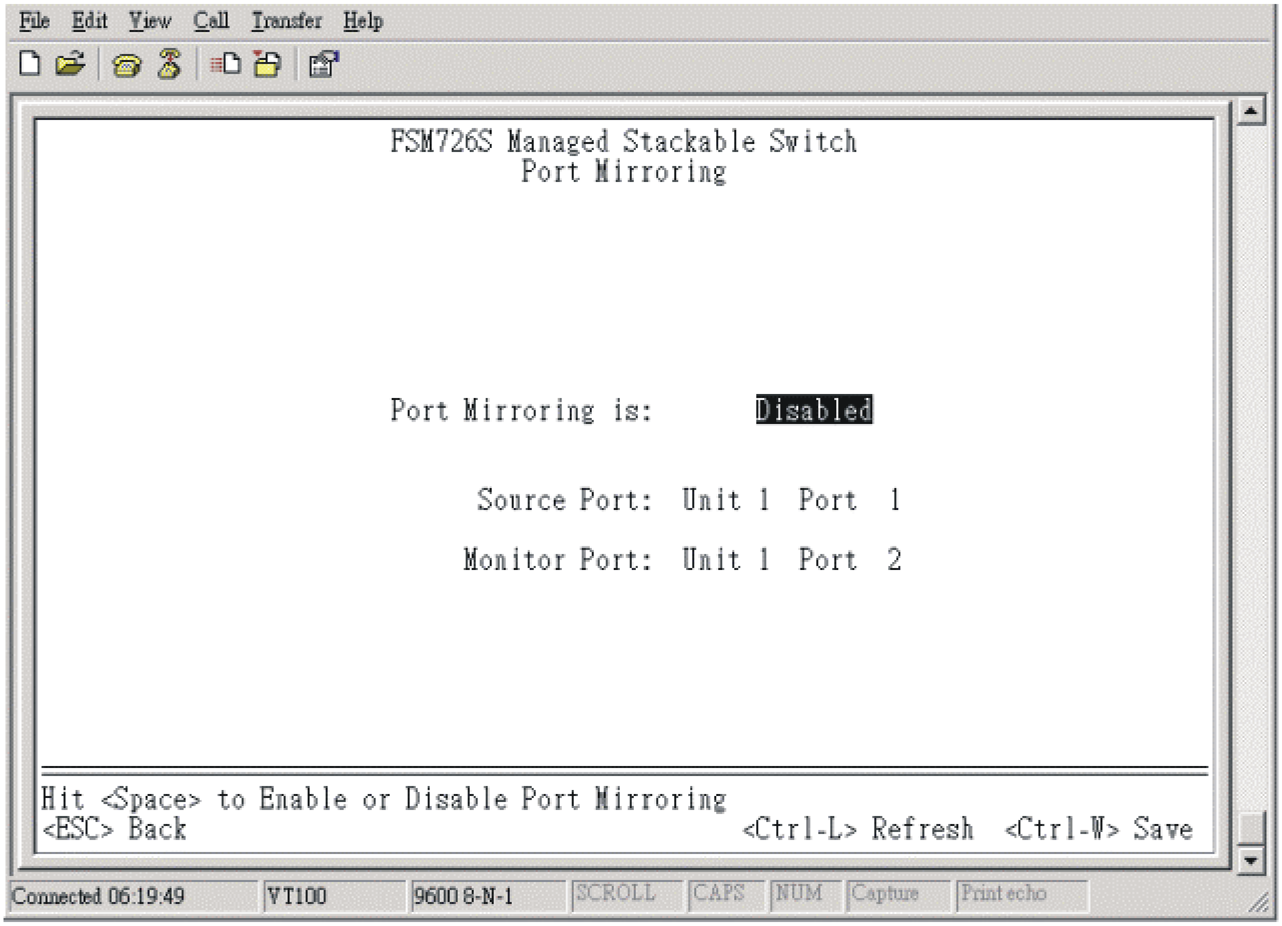
Main Menu> Advanced Menu

There are 8 sub-menus here.

- Port Mirroring
- Port Trunking
- Multimedia Support (IGMP)
- Traffic Prioritization
- VLAN
- Spanning Tree
- MAC Address Manager
- SNMP

Main Menu> Advanced Menu> Port Mirroring

This menu option allows you to enable the Port Mirroring capability (see Figure 6-13). You need to specify both the Source and Monitor port. The Monitor port will show a copy of every packet that arrives and departs at the Source port.



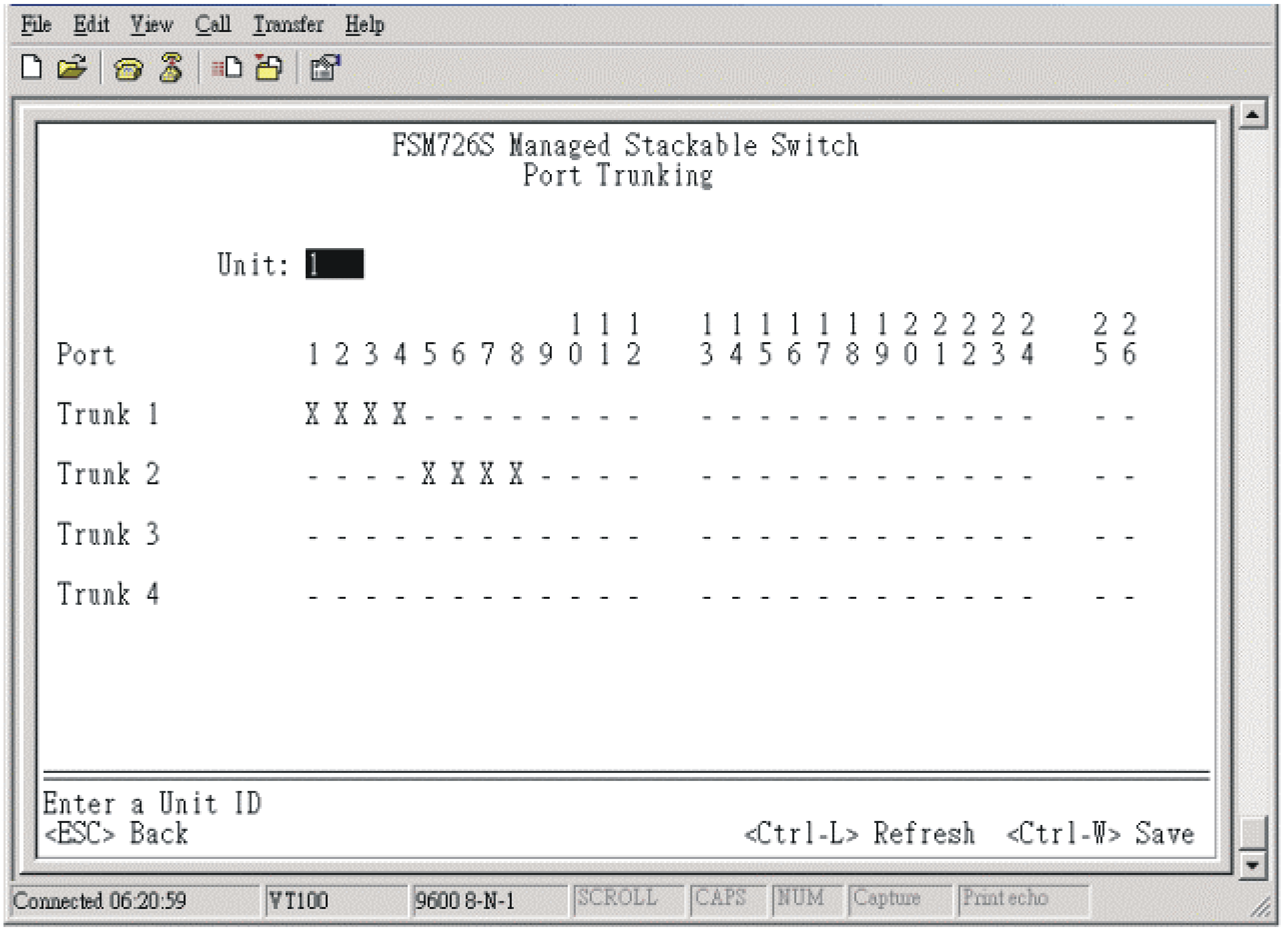
```
                    FSM726S Managed Stackable Switch
                             Port Mirroring



                    Port Mirroring is:      Disabled

                          Source Port:  Unit 1  Port  1

                         Monitor Port:  Unit 1  Port  2



Hit <Space> to Enable or Disable Port Mirroring
<ESC> Back                                <Ctrl-L> Refresh  <Ctrl-W> Save
```

Figure 6-13: Port Mirroring

Main Menu> Advanced Menu> Port Trunking

Port Trunking is a feature that allows multiple links between switches to work as one virtual link or aggregate link. Trunks can be defined for similar port types only. For example, a 10/100 port cannot form a Port Trunk with a gigabit port. For 10/100 ports, trunks can only be formed within the same bank. A bank is ports 1 to 8, ports 9 to 16, ports 17 to 24, or port 25 and port 26, on the same switch unit. Up to four trunks can be enabled at the same time within a stack. To set up a trunk, use the space bar to select the ports that will participate in the trunk. Spanning Tree will treat trunked ports as a single virtual port.

Note: you must use straight-though cables for all links in the trunk. Do not use crossover cables.
Note: you must disable auto-negotiation on the trunked ports???



```
                     FSM726S Managed Stackable Switch
                               Port Trunking


             Unit: 1

                                     1 1 1    1 1 1 1 1 1 1 2 2 2 2 2    2 2
Port                 1 2 3 4 5 6 7 8 9 0 1 2    3 4 5 6 7 8 9 0 1 2 3 4    5 6

Trunk 1              X X X X - - - - - - - -    - - - - - - - - - - - -    - -

Trunk 2              - - - - X X X X - - - -    - - - - - - - - - - - -    - -

Trunk 3              - - - - - - - - - - - -    - - - - - - - - - - - -    - -

Trunk 4              - - - - - - - - - - - -    - - - - - - - - - - - -    - -



Enter a Unit ID
<ESC> Back                                  <Ctrl-L> Refresh  <Ctrl-W> Save
```

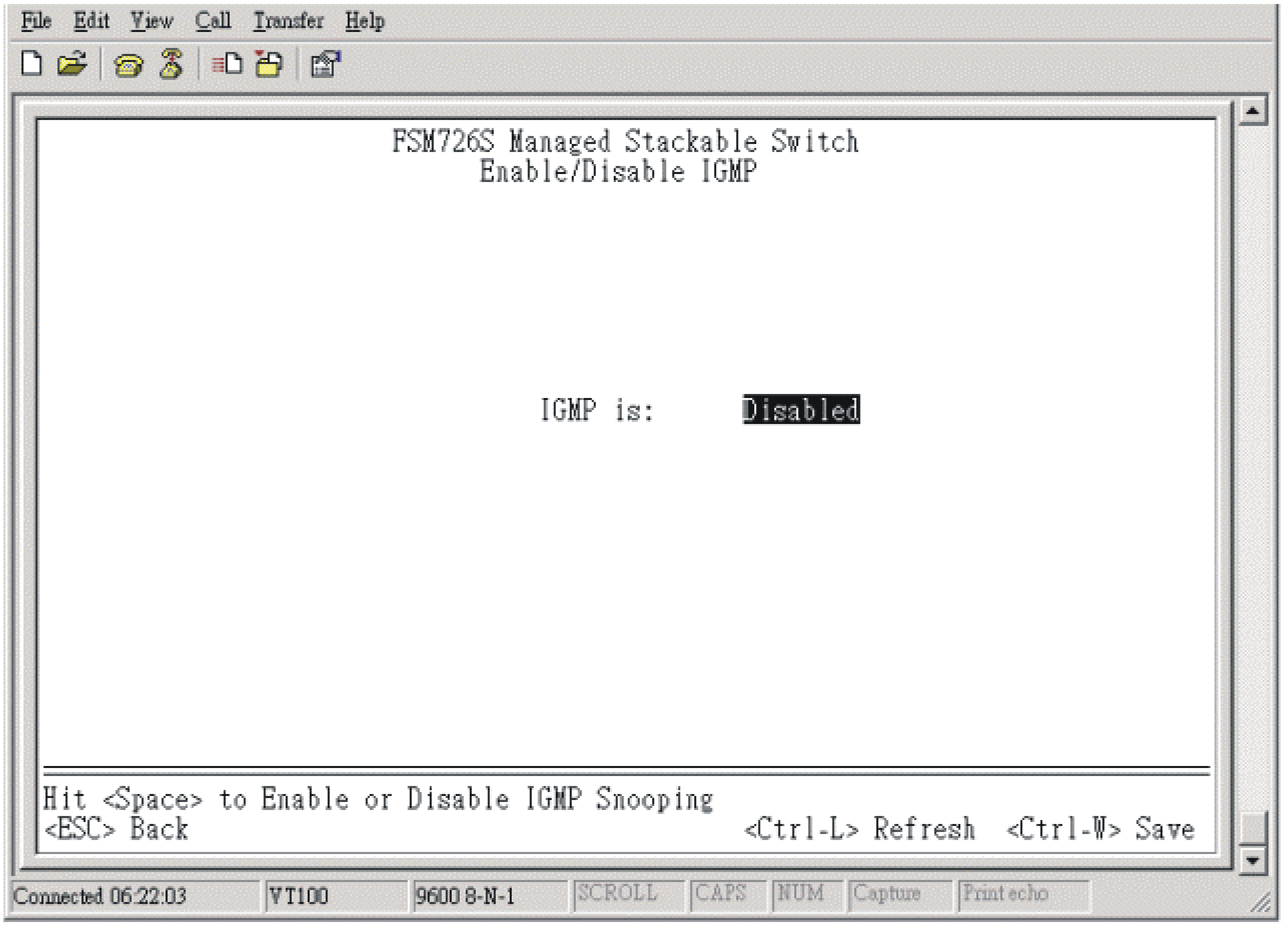
Figure 6-14: Port Trunking

Main Menu> Advanced Menu> Enable/Disable IGMP

In networks where multimedia applications generate multicast traffic, Internet Group Multicast Protocol (IGMP) can greatly reduce unnecessary bandwidth usage by limiting traffic forwarding that is otherwise broadcast to the whole network. Enabling IGMP will allow individual ports to detect IGMP queries, report packets, and manage IP multicast traffic through the switch.

IGMP

- Enable The system will detect IGMP queries, report packets, and manage IP multicast traffic through the switch
- Disable The switch will forward traffic and disregard any IGMP requests.

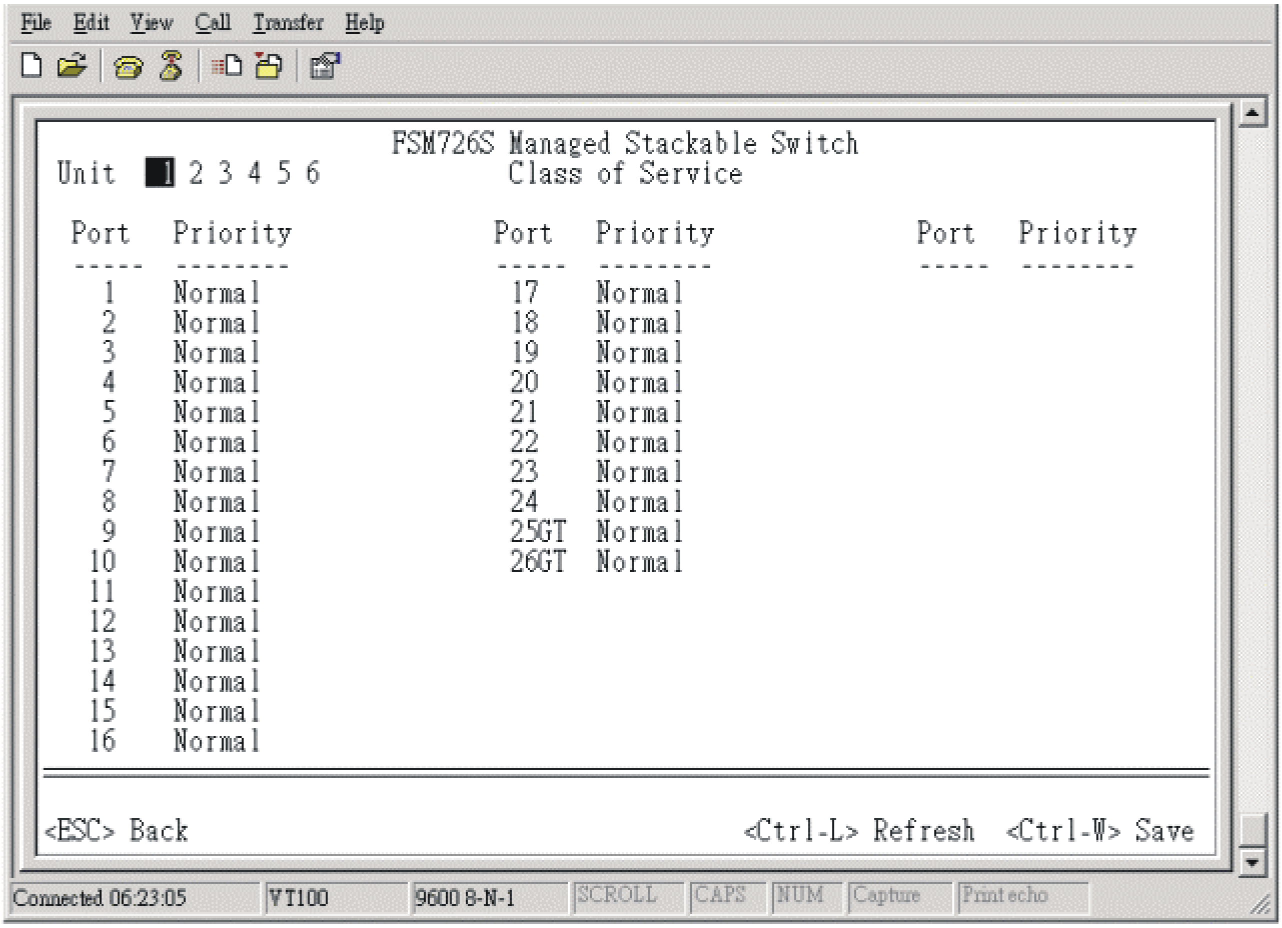


```
                    FSM726S Managed Stackable Switch
                          Enable/Disable IGMP



                      IGMP is:      Disabled



Hit <Space> to Enable or Disable IGMP Snooping
<ESC> Back                              <Ctrl-L> Refresh  <Ctrl-W> Save
```

Figure 6-15: Multimedia Support (IGMP)

Main Menu> Advanced Menu> CoS

Port Priority allows the user to specify which ports have greater precedence in situations where traffic may be buffered in the switch due to congestion. The ports with a setting of ‘high’ will transmit their packets before those with a ‘normal’ setting. The settings on this page only affect ingress packets that are not already tagged for priority. To raise the priority of a given port, toggle the port’s setting from ‘normal’ to ‘high’. The default and normal setting for a port is ‘normal’.



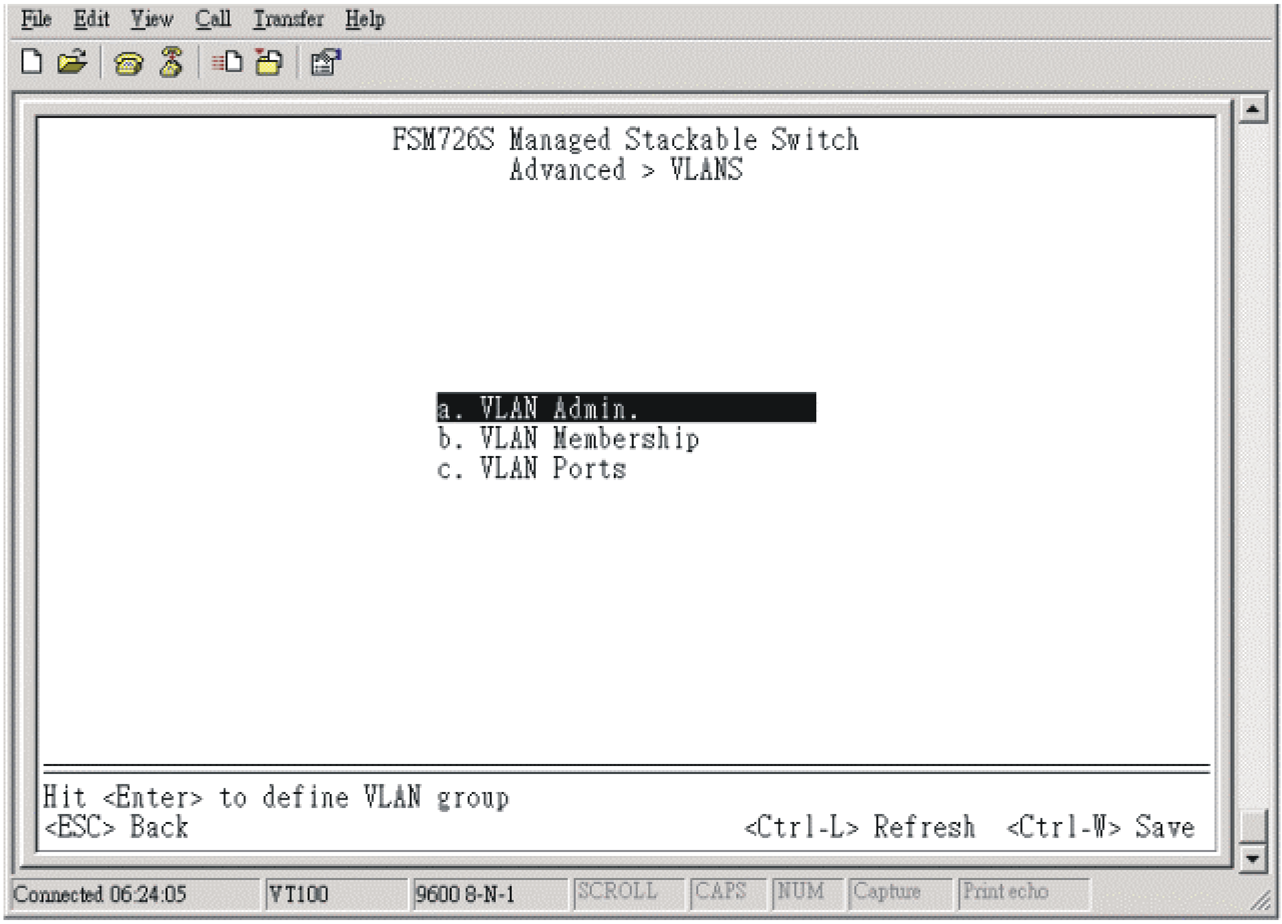
```
                        FSM726S Managed Stackable Switch
Unit  1 2 3 4 5 6               Class of Service

 Port   Priority            Port   Priority            Port   Priority
 -----  --------            -----  --------            -----  --------
   1    Normal               17    Normal
   2    Normal               18    Normal
   3    Normal               19    Normal
   4    Normal               20    Normal
   5    Normal               21    Normal
   6    Normal               22    Normal
   7    Normal               23    Normal
   8    Normal               24    Normal
   9    Normal               25GT  Normal
  10    Normal               26GT  Normal
  11    Normal
  12    Normal
  13    Normal
  14    Normal
  15    Normal
  16    Normal

<ESC> Back                                    <Ctrl-L> Refresh  <Ctrl-W> Save
```

Figure 6-16: Class of Service

Main Menu> Advanced Menu> VLAN Setup

A Virtual Local Area Network (VLAN) is a means to electronically separate ports on the same switch from a single broadcast domain into separate broadcast domains. By using VLAN, users can group by logical function instead of physical location. This switch supports up to 64VLANs. This switch supports static, port-based VLANs.

The VLAN Setup options are as follows:



```
                     FSM726S Managed Stackable Switch
                            Advanced > VLANS



                 a. VLAN Admin.
                 b. VLAN Membership
                 c. VLAN Ports



Hit <Enter> to define VLAN group
<ESC> Back                                 <Ctrl-L> Refresh  <Ctrl-W> Save
```

Figure 6-17: VLAN Set-up

Main Menu> Advanced Menu> VLANS Setup> VLAN Admin

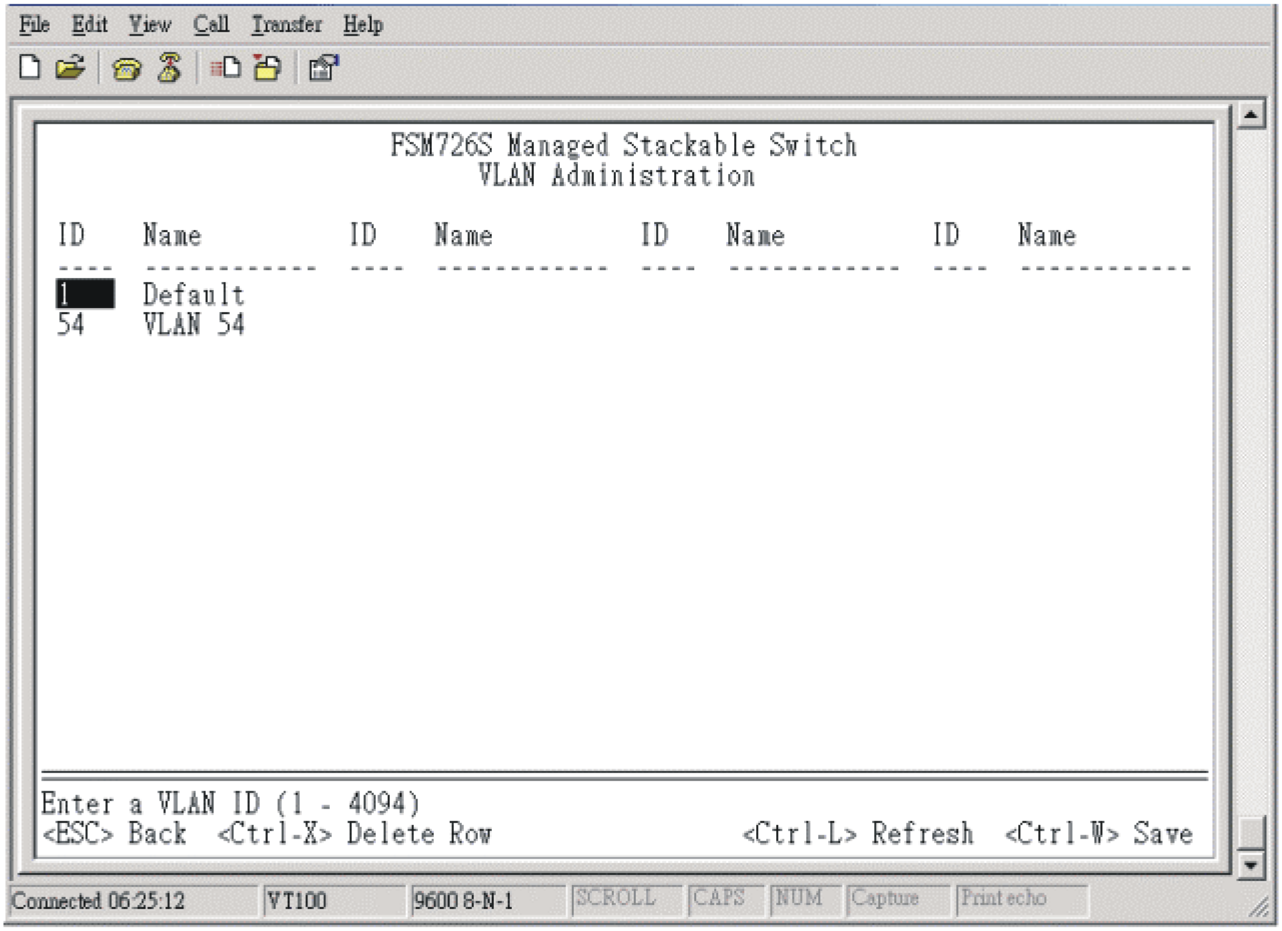
Up to 64 VLANs with unique ID numbers and names can be added. VLAN ID numbers must be in the range of 1-4094.

Add a VLAN

1. Type a unique numeric VLAN ID and hit Enter
2. Type a unique VLAN name and hit Enter

Remove a port or an entire VLAN

To remove an entire VLAN, just press Ctrl-X anywhere on that line



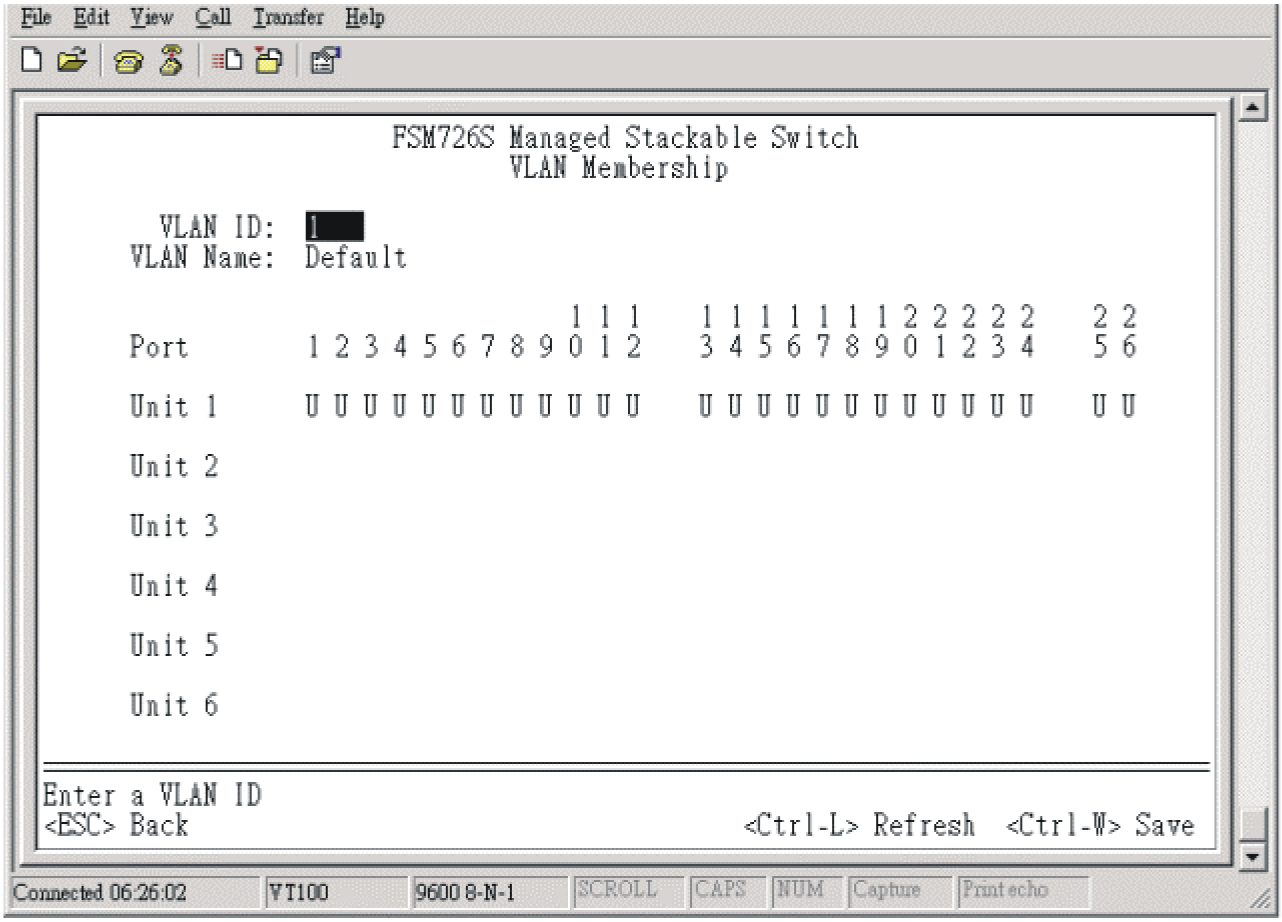
```
                     FSM726S Managed Stackable Switch
                          VLAN Administration

ID    Name          ID    Name          ID    Name          ID    Name
----  ------------  ----  ------------  ----  ------------  ----  ------------
1     Default
54    VLAN 54

Enter a VLAN ID (1 - 4094)
<ESC> Back  <Ctrl-X> Delete Row                 <Ctrl-L> Refresh  <Ctrl-W> Save
```

Figure 6-18: VLAN Administration

Main Menu> Advanced Menu> VLANS Setup> VLAN Membership

This matrix allows for real time management of up to 64 VLANs. To add a port to a VLAN, position the cursor in the desired matrix location and toggle the options with the SPACE bar.

A 'U' or 'T' will be displayed for each port assigned to the VLAN (see Figure 6-20), where 'U' stands for untagged and 'T' for tagged. A '_' space indicates that the port is not a member of the particular VLAN. VLAN tagging is a standard set by the IEEE to facilitate the spanning of VLANs across multiple switches. (Reference: Appendix C and IEEE Std 802.1Q-1998 Virtual Bridged Local Area Networks)

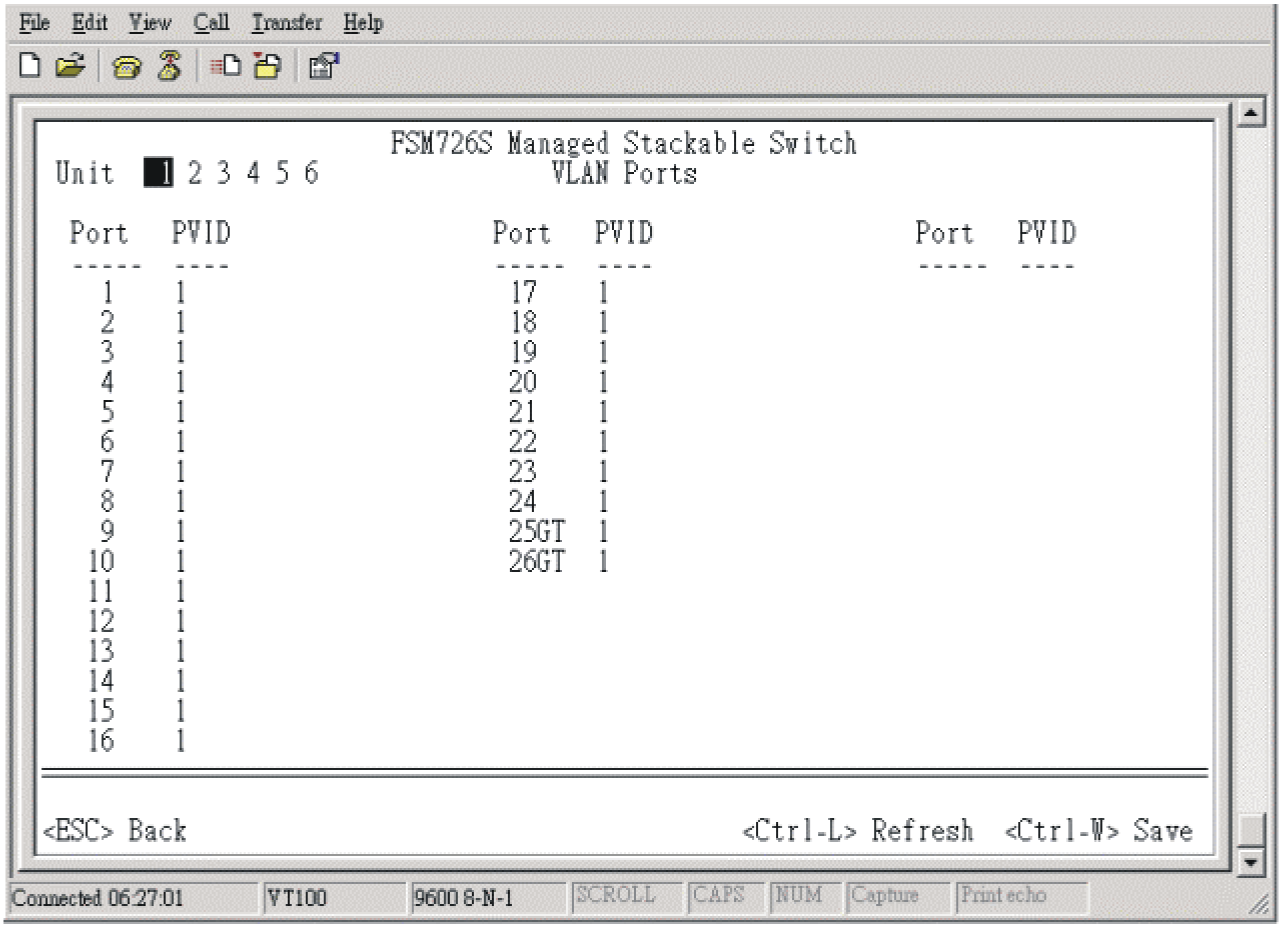


```
                      FSM726S Managed Stackable Switch
                              VLAN Membership

      VLAN ID:   1
    VLAN Name:   Default

                                   1 1 1   1 1 1 1 1 1 1 2 2 2 2 2   2 2
    Port         1 2 3 4 5 6 7 8 9 0 1 2   3 4 5 6 7 8 9 0 1 2 3 4   5 6

    Unit 1       U U U U U U U U U U U U   U U U U U U U U U U U U   U U

    Unit 2

    Unit 3

    Unit 4

    Unit 5

    Unit 6

Enter a VLAN ID
<ESC> Back                               <Ctrl-L> Refresh  <Ctrl-W> Save
```

Figure 6-19: VLAN Membership

Main Menu> Advanced Menu> VLANS Setup> VLAN Ports

All untagged packets entering the switch will by default be tagged with the ID specified by the port's PVID. This screen allows you to specify the PVID for each port. An 'X' in the Port VLAN ID Setup page will mark which PVID is set for each port

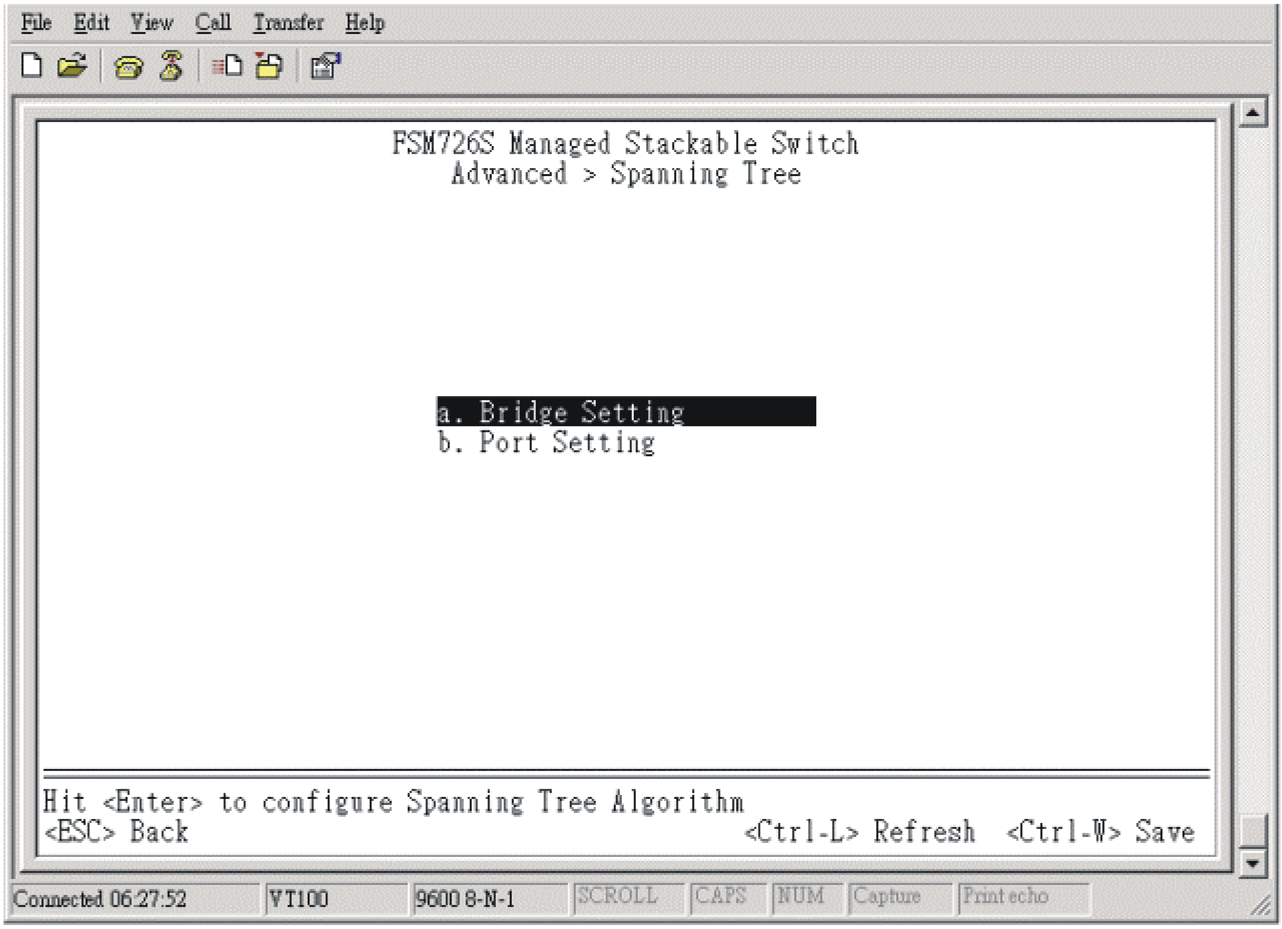


```
                         FSM726S Managed Stackable Switch
Unit  1 2 3 4 5 6                    VLAN Ports

 Port   PVID                 Port   PVID                 Port   PVID
 -----  ----                 -----  ----                 -----  ----
   1    1                     17    1
   2    1                     18    1
   3    1                     19    1
   4    1                     20    1
   5    1                     21    1
   6    1                     22    1
   7    1                     23    1
   8    1                     24    1
   9    1                     25GT  1
  10    1                     26GT  1
  11    1
  12    1
  13    1
  14    1
  15    1
  16    1

<ESC> Back                                   <Ctrl-L> Refresh  <Ctrl-W> Save
```

Figure 6-20: PVID Settings

Main Menu> Advanced Menu> Spanning Tree

This switch is compliant with IEEE802.1D Spanning Tree Protocol (STP). STP ensures that only one path at a time is active between any two network nodes. There are maybe more than two physical path between any two nodes for redundant paths; STP ensures only one physical path is active and the others are blocked. STP will prevent an inadvertent loop in a network, which can disable your network due to a "Broadcast storm", the result of a broadcast message traveling through the loop again and again.



```
                  FSM726S Managed Stackable Switch
                     Advanced > Spanning Tree



                        a. Bridge Setting
                        b. Port Setting



Hit <Enter> to configure Spanning Tree Algorithm
<ESC> Back                              <Ctrl-L> Refresh  <Ctrl-W> Save
```

Figure 6-21: Spanning Tree

Main Menu> Advanced Menu> Spanning Tree> Bridge Settings

The following information is presented on the this page:

- Root Port
- Root Port Path Cost
- Bridge Hello Time
- Bridge Max Age
- Bridge Forward Delay
- Root Bridge Priority
- Root MAC Address
- Switch MAC Address

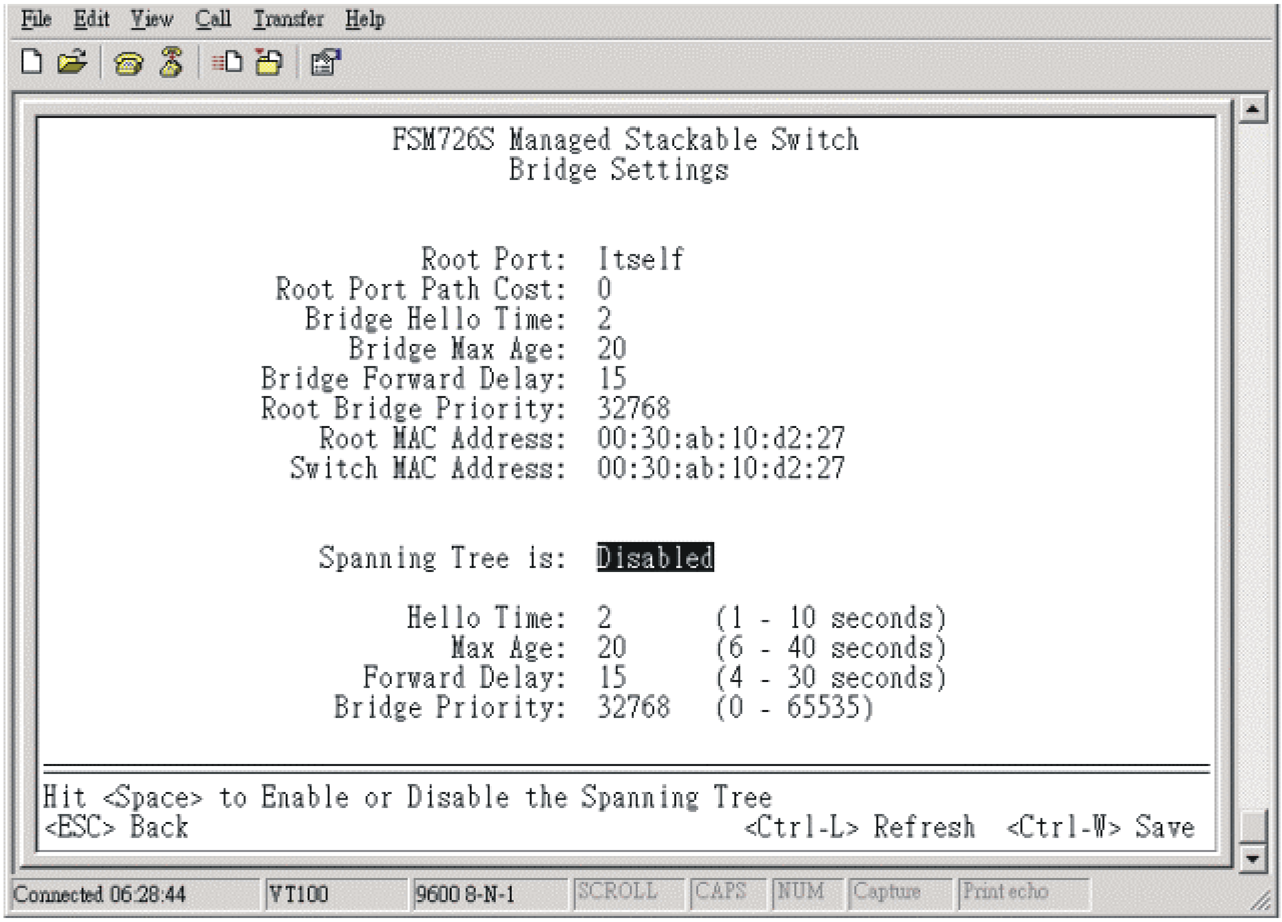
Spanning Tree can be enabled or disabled in this screen.

Enable: There are four other tunable parameters to be addressed when enabled.

Hello Time	Time between configuration messages sent by the Spanning Tree algorithm
Max Age	Amount of time before a configuration message is discarded by the system
Forward Delay	Amount of time system spent transitioning from the ‘learning’ to the ‘listening’ to the ‘forwarding’ states
Bridge Priority	Priority setting among other switches in the Spanning Tree

Disable: Disable Spanning Tree algorithm on the system.

When Spanning tree is used in conjunction with a set of aggregated ports, otherwise known as a port trunking, Spanning Tree will treat the trunk as a single virtual port.



```
                    FSM726S Managed Stackable Switch
                            Bridge Settings


                  Root Port:  Itself
        Root Port Path Cost:  0
          Bridge Hello Time:  2
             Bridge Max Age:  20
       Bridge Forward Delay:  15
       Root Bridge Priority:  32768
           Root MAC Address:  00:30:ab:10:d2:27
         Switch MAC Address:  00:30:ab:10:d2:27


           Spanning Tree is:  Disabled

                 Hello Time:  2        (1 - 10 seconds)
                    Max Age:  20       (6 - 40 seconds)
              Forward Delay:  15       (4 - 30 seconds)
            Bridge Priority:  32768    (0 - 65535)

Hit <Space> to Enable or Disable the Spanning Tree
<ESC> Back                                 <Ctrl-L> Refresh  <Ctrl-W> Save
```

Figure 6-22: Spanning Tree: Bridge Settings

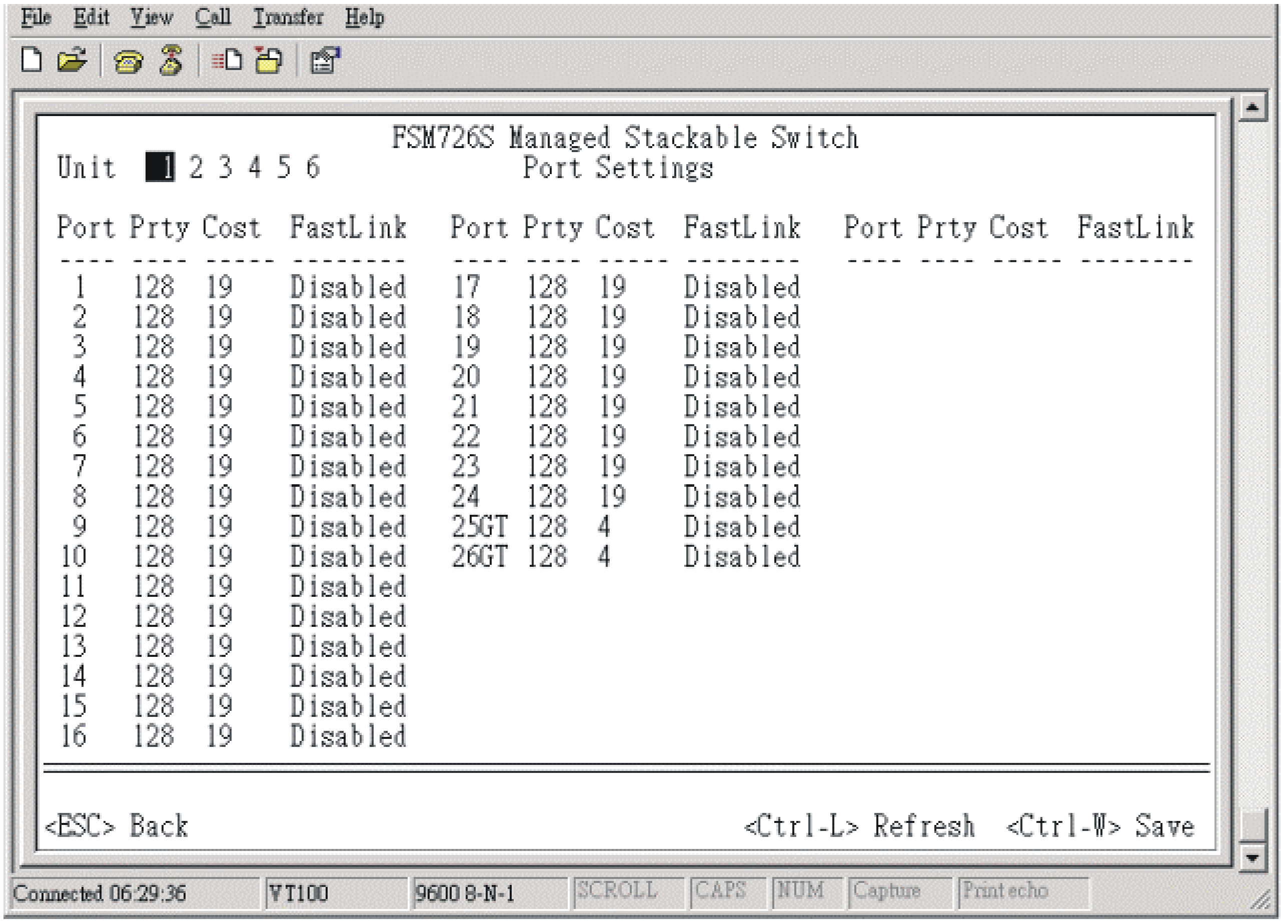
Main Menu> Advanced Menu> Spanning Tree> Port Settings

For the Port Settings options, you can specify Spanning Tree parameters for each port. These parameters include port priority, path cost, and Fastlink.

Table 6-1 STP Port Setting Parameters

Parameters	Range	Description
Prty (Priority)	0-255	STP bases on this to determine the port to use for forwarding. The port with the lowest number has the highest priority.
Cost	1-65535	The switch uses this to determine which port is the forwarding port. All other factors equal, the path with the lowest cost to the root bridge will be the active path.

Fastlink in STP mode
When a port running the standard STP is connected, it will go through the STP negotiation (listening -> learning -> forwarding or blocking) before it will be fully available. If a server is trying to access a client through the switch running the STP negotiation, it will not be able to connect to it immediately. This can be a problem for some networks. Fastlink mode solves this problem by setting the port directly to forwarding mode, thus allowing any server access request to be forwarded. Fastlink mode can cause temporary loops in your network, but the STP will find and eliminate them. Fastlink is best used on end node ports, i.e. ports connected to PCs or servers, to avoid network loops.



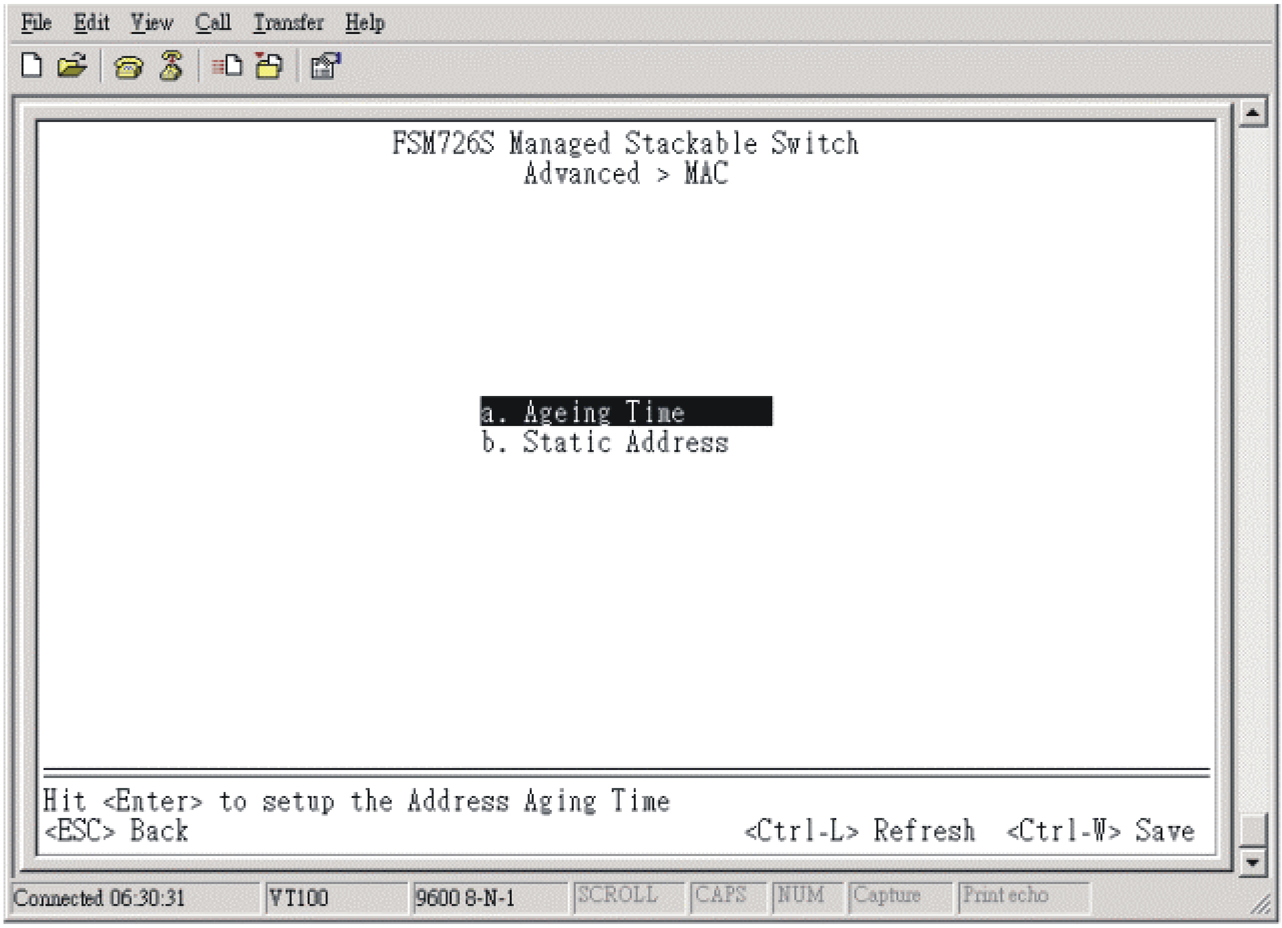
```
                        FSM726S Managed Stackable Switch
Unit  1 2 3 4 5 6                 Port Settings

Port Prty Cost  FastLink   Port Prty Cost  FastLink   Port Prty Cost  FastLink
---- ---- ----- --------   ---- ---- ----- --------   ---- ---- ----- --------
 1   128  19    Disabled   17   128  19    Disabled
 2   128  19    Disabled   18   128  19    Disabled
 3   128  19    Disabled   19   128  19    Disabled
 4   128  19    Disabled   20   128  19    Disabled
 5   128  19    Disabled   21   128  19    Disabled
 6   128  19    Disabled   22   128  19    Disabled
 7   128  19    Disabled   23   128  19    Disabled
 8   128  19    Disabled   24   128  19    Disabled
 9   128  19    Disabled   25GT 128  4     Disabled
10   128  19    Disabled   26GT 128  4     Disabled
11   128  19    Disabled
12   128  19    Disabled
13   128  19    Disabled
14   128  19    Disabled
15   128  19    Disabled
16   128  19    Disabled

<ESC> Back                                 <Ctrl-L> Refresh  <Ctrl-W> Save
```

Figure 6-23: Spanning Tree: Port Settings

Main Menu> Advanced Menu> MAC Address Manager

There are two advanced setup parameter can be configured here.

- Static Address
- Address Aging

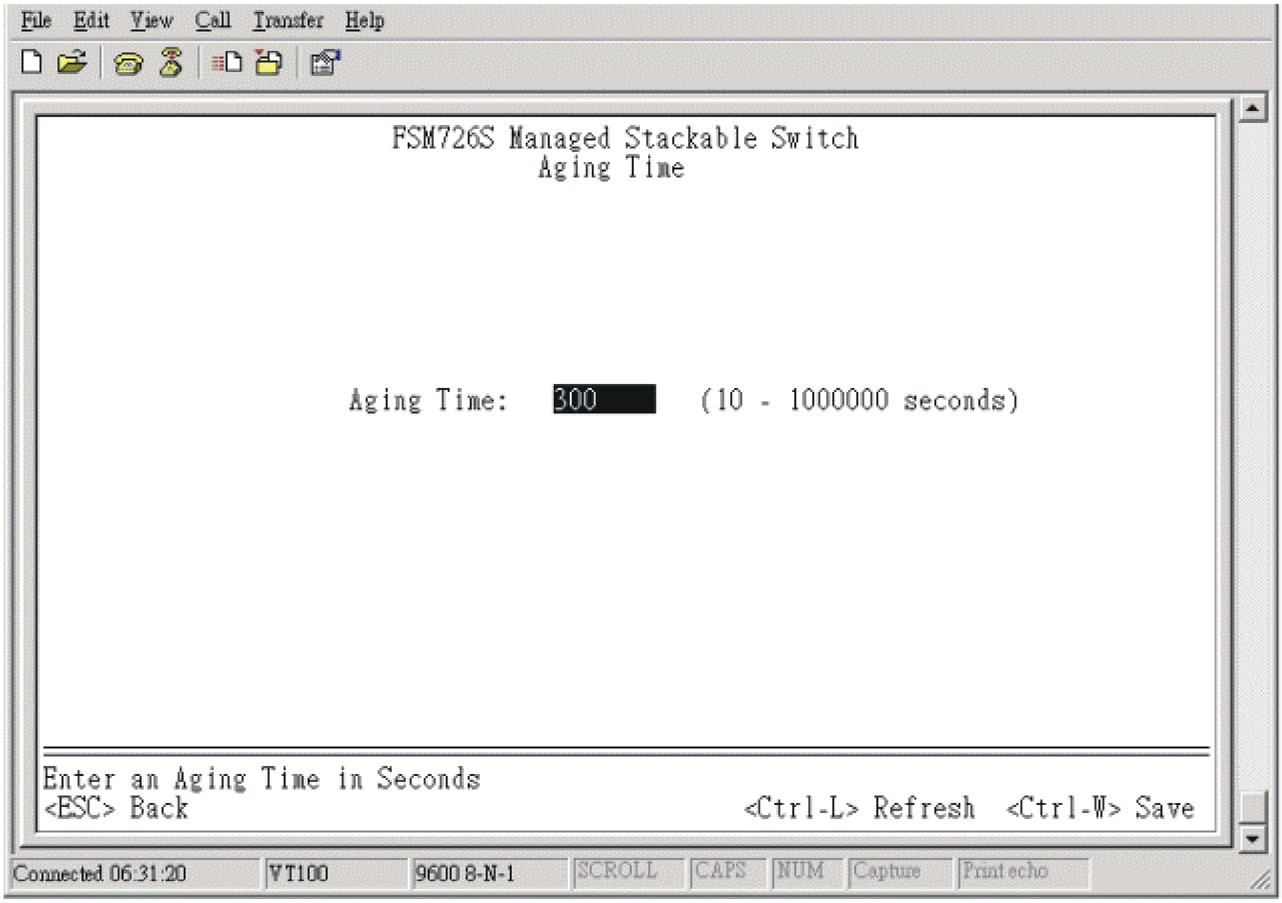


```
FSM726S Managed Stackable Switch
        Advanced > MAC



       a. Ageing Time
       b. Static Address

Hit <Enter> to setup the Address Aging Time
<ESC> Back                                   <Ctrl-L> Refresh  <Ctrl-W> Save
```

Figure 6-24: Address Manager

Main Menu> Advanced Menu> MAC Address Manager> Address Aging

The aging time is the amount of time that an entry is kept in the bridge tables prior to being purged (or aged). The range (in parentheses) represents the minimum and the maximum values that the timer can be set.



```
FSM726S Managed Stackable Switch
           Aging Time

Aging Time:   300       (10 - 1000000 seconds)

Enter an Aging Time in Seconds
<ESC> Back                          <Ctrl-L> Refresh  <Ctrl-W> Save
```

Figure 6-25: Address Manager: Address Aging

Main Menu> Advanced Menu> MAC Address Manager> Static Addresses

The Static Addresses Table, allows the administrator to specify Media Access Control (MAC) addresses for specific ports that will not be purged from the bridge table by the aging function.

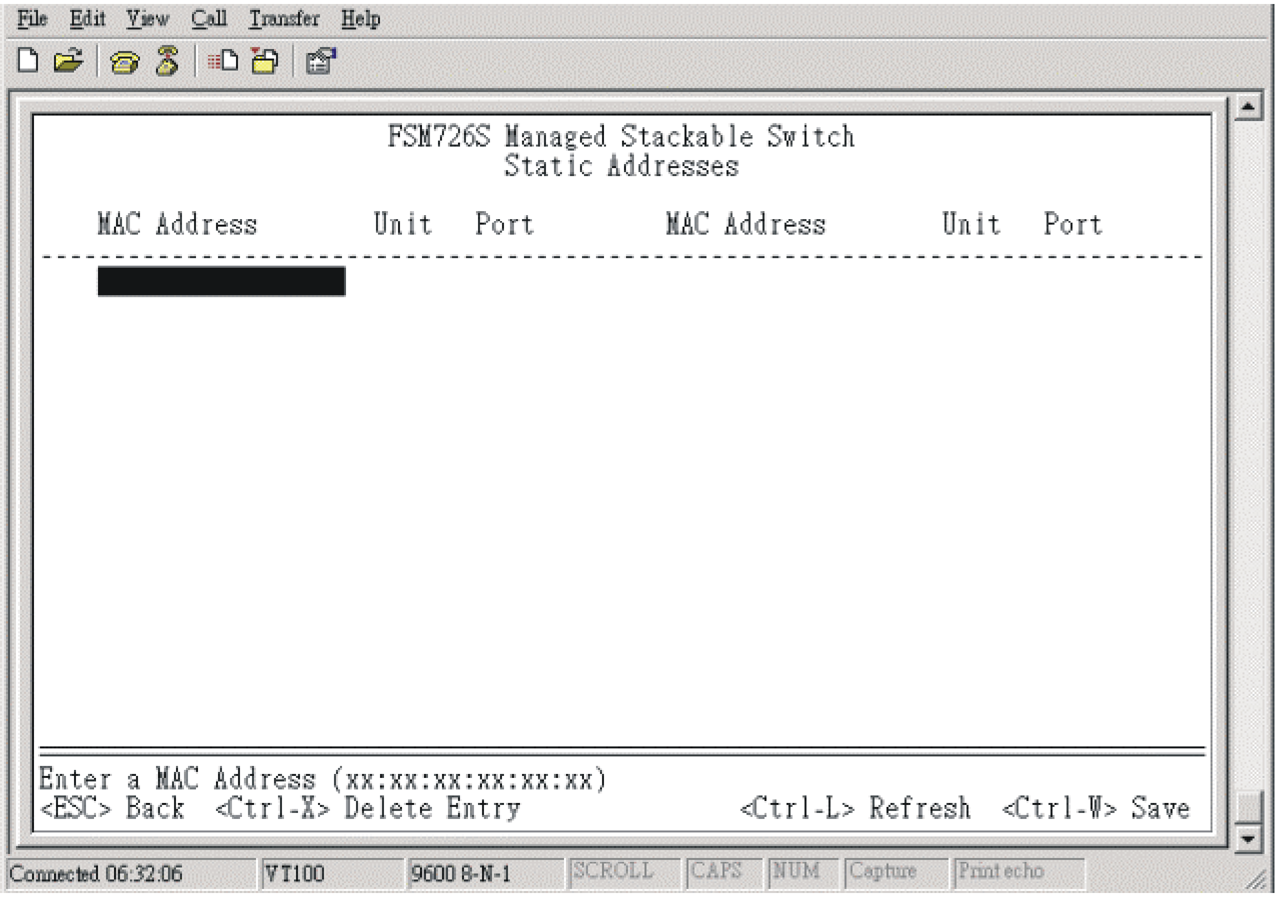
Add an entry

- Type the MAC address under the first column, and hit Enter.
- Enter the port number, which is associated with the MAC address.

If all the information is correct, the new entry will appear in the list below, which is in order by port ID. Otherwise, an error message will be displayed and the cursor will return to the MAC Address field.

Remove an entry

- Tab down to the entry and press Ctrl-X. ESC will return to the previous menu.



```
                     FSM726S Managed Stackable Switch
                            Static Addresses

   MAC Address         Unit   Port          MAC Address         Unit   Port
 ---------------------------------------------------------------------------



 Enter a MAC Address (xx:xx:xx:xx:xx:xx)
 <ESC> Back  <Ctrl-X> Delete Entry                 <Ctrl-L> Refresh  <Ctrl-W> Save
```

Figure 6-26: Address Manager: Static Addresses

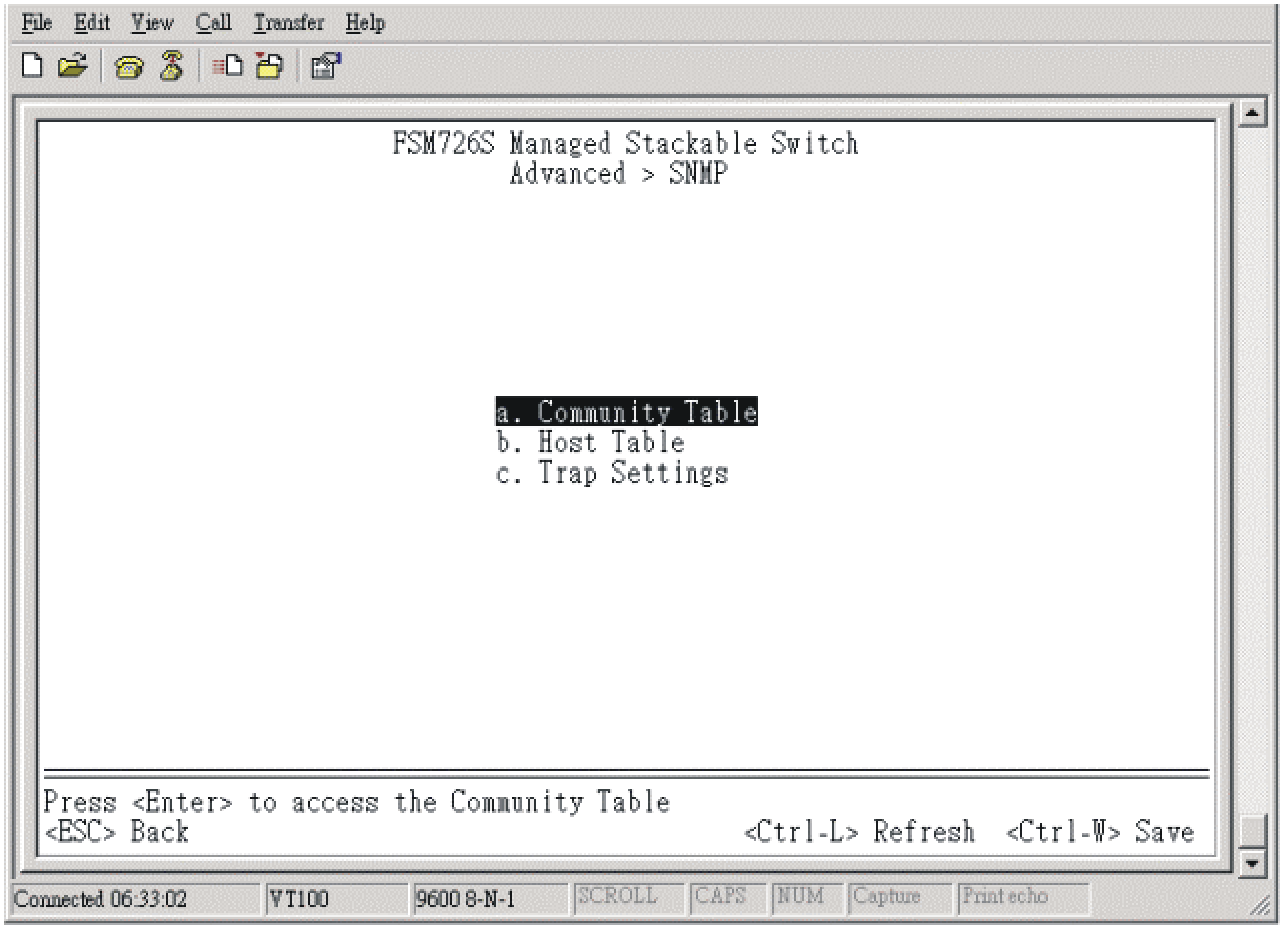
Main Menu> Advanced Menu> SNMP

You can manage this switch by SNMP from a network management station.
SNMP management features on the switch include:

- Simple Network Management Protocol (SNMP)
- Support Standard MIBs:
  - MIB II (RFC1213)
  - Ethernet Interface MIB (RFC1643)
  - Bridge MIB (RFC1493)
  - Private Enterprise MIB
  - 4-Group RMON (RFC1757)

This page has three options:

- Community Table
- Host Table
- Trap Setting

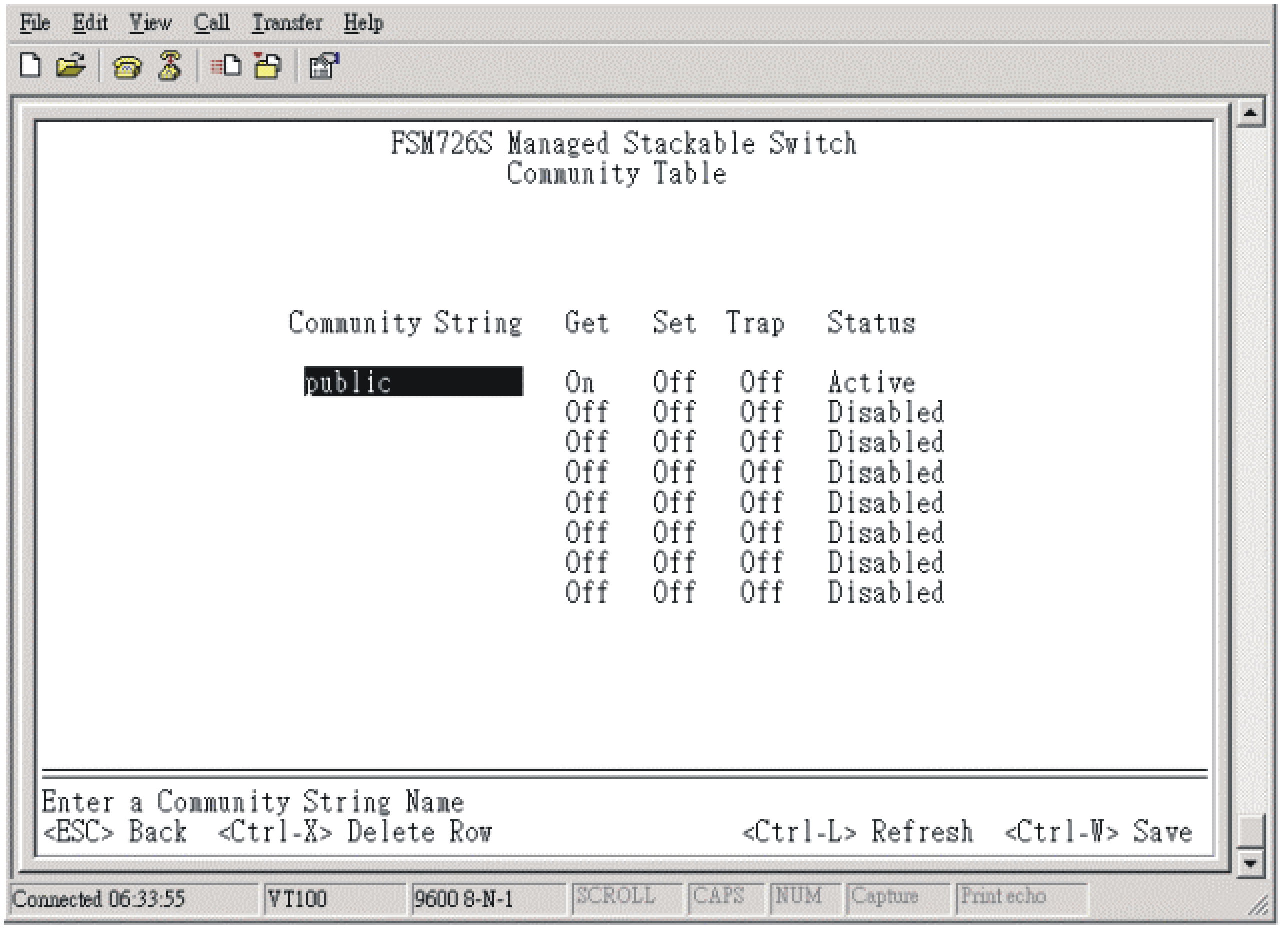


```
FSM726S Managed Stackable Switch
      Advanced > SNMP

        a. Community Table
        b. Host Table
        c. Trap Settings

Press <Enter> to access the Community Table
<ESC> Back                           <Ctrl-L> Refresh  <Ctrl-W> Save
```

Figure 6-27: SNMP Management

Main Menu> Advanced Menu> SNMP> Community Table

You can create up to eight different community strings with combinations of GET, SET and TRAP privileges. These community strings need to be set prior to setting host access, as the host table depends on the existence of community strings. The public string has GET privileges by default.



```
                 FSM726S Managed Stackable Switch
                          Community Table



         Community String    Get   Set   Trap   Status

          public             On    Off   Off    Active
                             Off   Off   Off    Disabled
                             Off   Off   Off    Disabled
                             Off   Off   Off    Disabled
                             Off   Off   Off    Disabled
                             Off   Off   Off    Disabled
                             Off   Off   Off    Disabled
                             Off   Off   Off    Disabled


Enter a Community String Name
<ESC> Back  <Ctrl-X> Delete Row               <Ctrl-L> Refresh  <Ctrl-W> Save
```

Figure 6-28: SNMP Management: Community Table

Main Menu> Advanced Menu> SNMP> Host Table

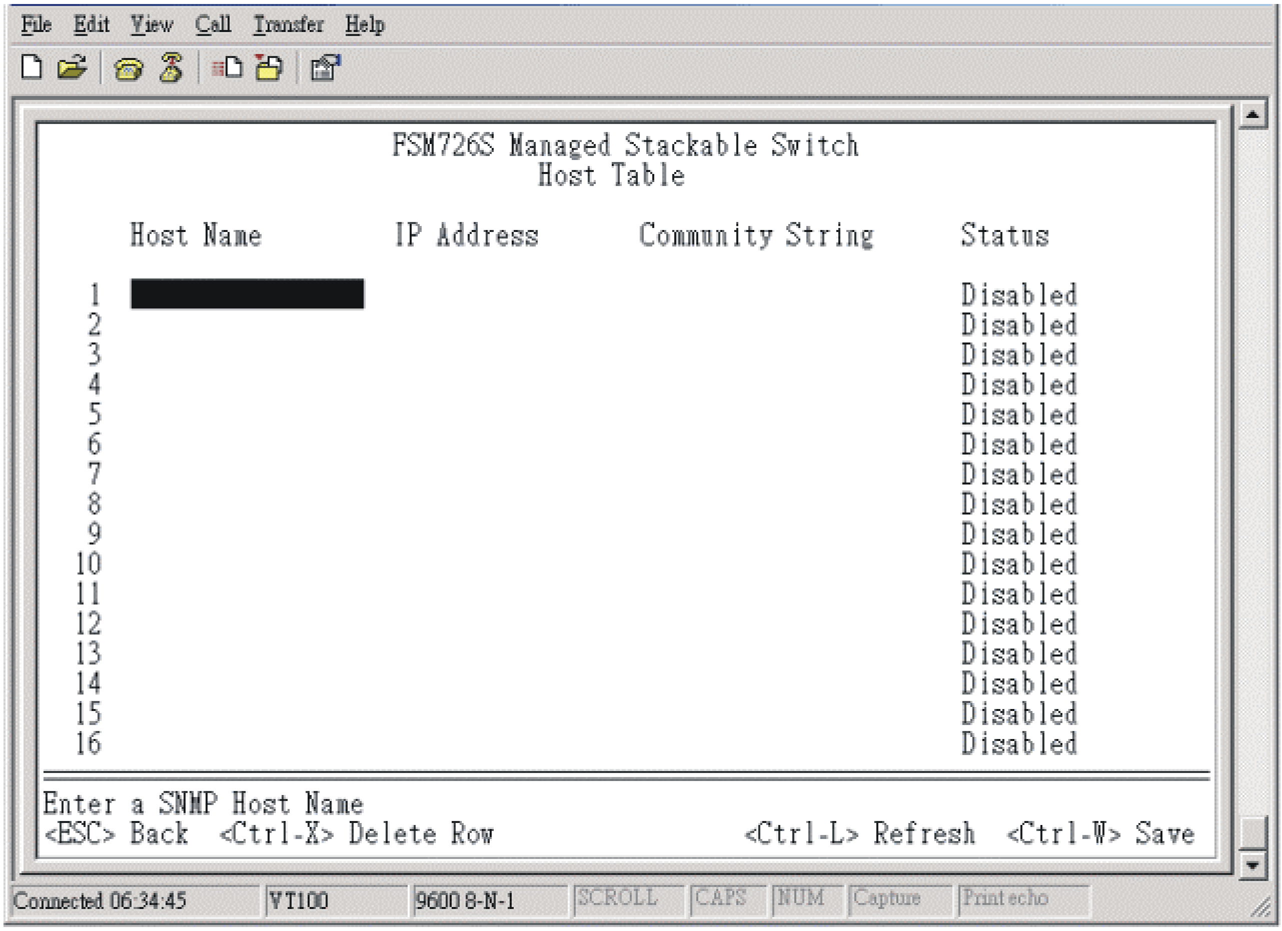
The screen, shown in Figure 6-29, grants a host the access rights to the switch.

Host Authorization must be enabled to use the host table. Host Authorization is used as a security feature to limit people who are not listed in the host table from accessing the switch.

If Host Authorization is enabled, the host must be added to this table, through the Console port connection in order for an end station to be access the switch via SNMP.

<u>Add host</u>

- Enter the host name, IP address, and the community string. Press Enter after each entry to move to the next field.
- In the Status field, press the Spacebar until the desired Status is displayed.
- Press Ctrl-W to save all changes.

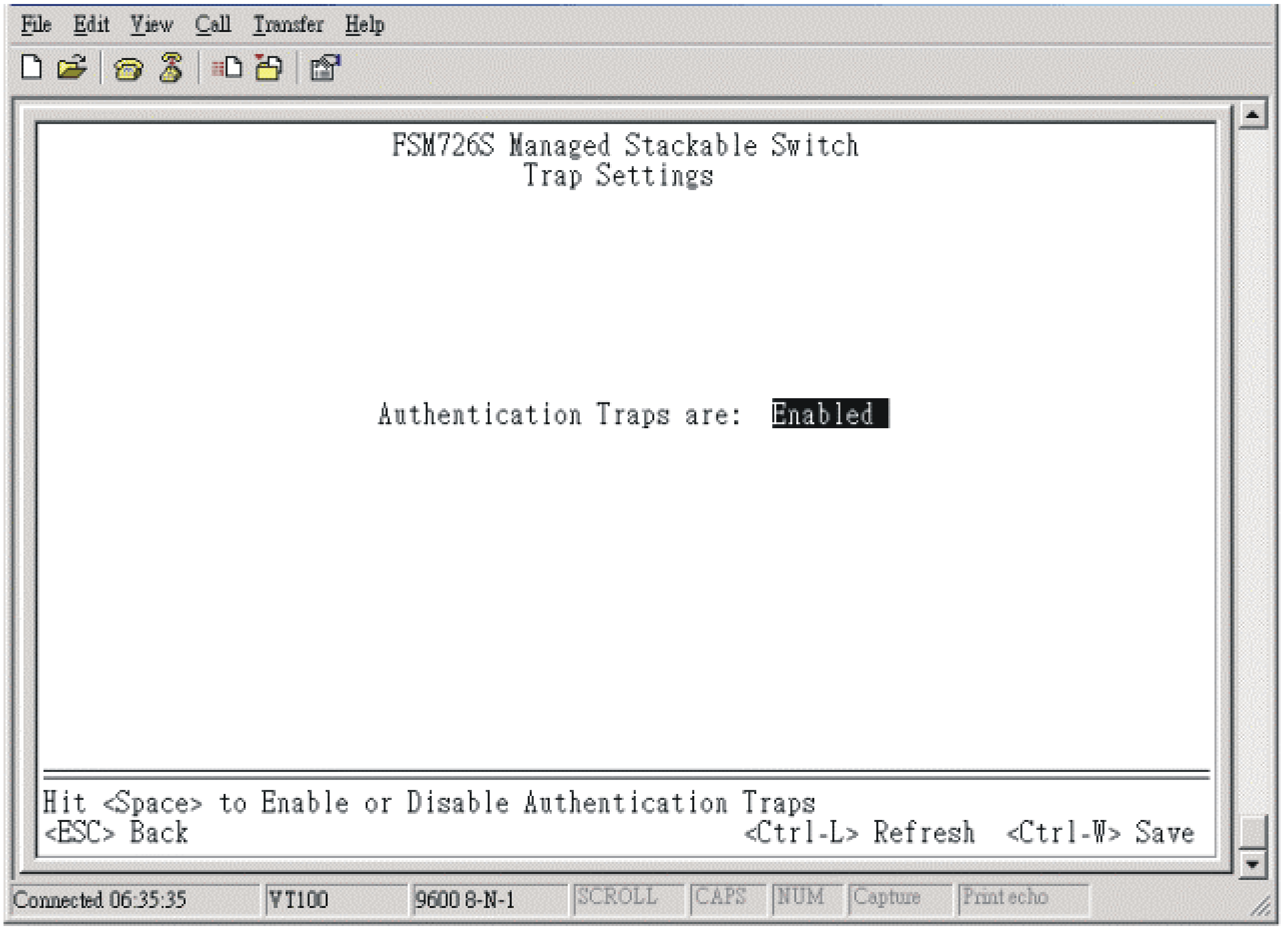


```
                    FSM726S Managed Stackable Switch
                               Host Table

      Host Name          IP Address        Community String       Status

   1                                                              Disabled
   2                                                              Disabled
   3                                                              Disabled
   4                                                              Disabled
   5                                                              Disabled
   6                                                              Disabled
   7                                                              Disabled
   8                                                              Disabled
   9                                                              Disabled
  10                                                              Disabled
  11                                                              Disabled
  12                                                              Disabled
  13                                                              Disabled
  14                                                              Disabled
  15                                                              Disabled
  16                                                              Disabled
 ____________________________________________________________________________
 Enter a SNMP Host Name
 <ESC> Back  <Ctrl-X> Delete Row                 <Ctrl-L> Refresh  <Ctrl-W> Save
```

Figure 6-29: SNMP Management: Host Table

Main Menu> Advanced Menu> SNMP> Trap Settings

Authentication Traps
When on, the system will generate an SNMP trap upon a host authorization failure. This failure occurs when a host tries to gain access to the system but the host's IP is not in the SNMP host table.



```
                         FSM726S Managed Stackable Switch
                                  Trap Settings



                     Authentication Traps are:  Enabled


Hit <Space> to Enable or Disable Authentication Traps
<ESC> Back                                   <Ctrl-L> Refresh  <Ctrl-W> Save
```

Figure 6-30: SNMP Management: Trap Settings

CHAPTER 7: WEB MANAGEMENT ACCESS

Your NETGEAR Model FSM726S Managed Stackable Switch provides a built-in browser interface that lets you configure and manage it remotely using a standard Web browser such as Microsoft Internet Explorer or Netscape Navigator. This interface also allows for system monitoring of the Switch. The 'help' page will cover many of the basic functions and features of the switch and it's web interface.

When you configure the switch for the first time from the console, you can assign an IP address and subnet mask to the switch. Thereafter, you can access the switch's Web interface directly using your Web browser by entering the switch's IP address. In this way, you can use your Web browser to manage the switch from a central location, just as if you were directly connected to the switch's console port. Figure 7-1 shows this management method.

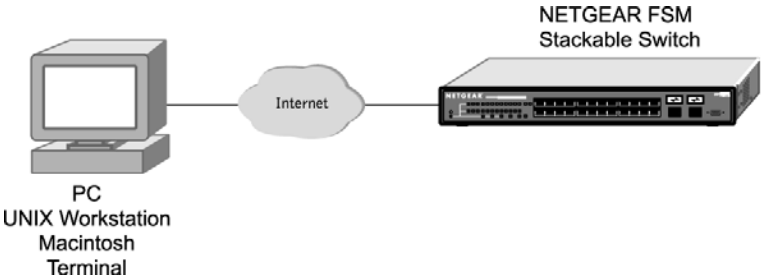
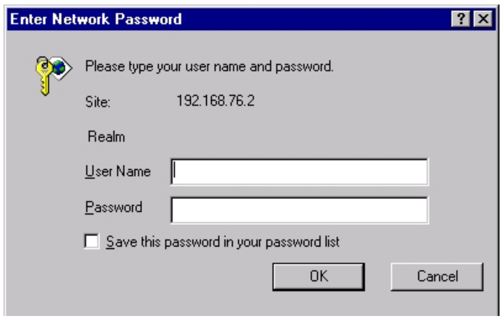


Figure 7-1. Web Management Method

Web Management requires either Microsoft Internet Explorer 5.0 or later or Netscape Navigator 6.0 or later.

Web Pages

Before connecting to the switch via a web browser (i.e. Netscape Navigator), a login screen will appear prompting for an administrator password (if the password protection is enabled). The User Name will always be 'admin'. Enter the password to access the switch's management mode. Once the password is entered correctly, the front page will appear.


Enter Network Password

Please type your user name and password.

Site: 192.168.76.2

Realm

User Name

Password

□ Save this password in your password list

Figure 7-2: Password

Note: If password protection is enabled (using the console) without setting your own password, the default password is '1234'.

There are 6 menu options available:

- System
- Status
- Set-up
- Tools
- Security
- Advanced

There is a help menu in the top of right side of screen; you can click the ‘help’ or the question mark to read the help menu.

The help menu contains:

Web-Based Management	Introduction to the Web management features.
Device Management	Introduction of the basic icons and management of the device
Interface Operations	Describes Web browser requirements, and common commands
Product Overview	Describes supported SNMP and Web management features
Summary of Features	Feature List

Within the various browser interface pages, there are several buttons that you can use. Their names and functions are below:

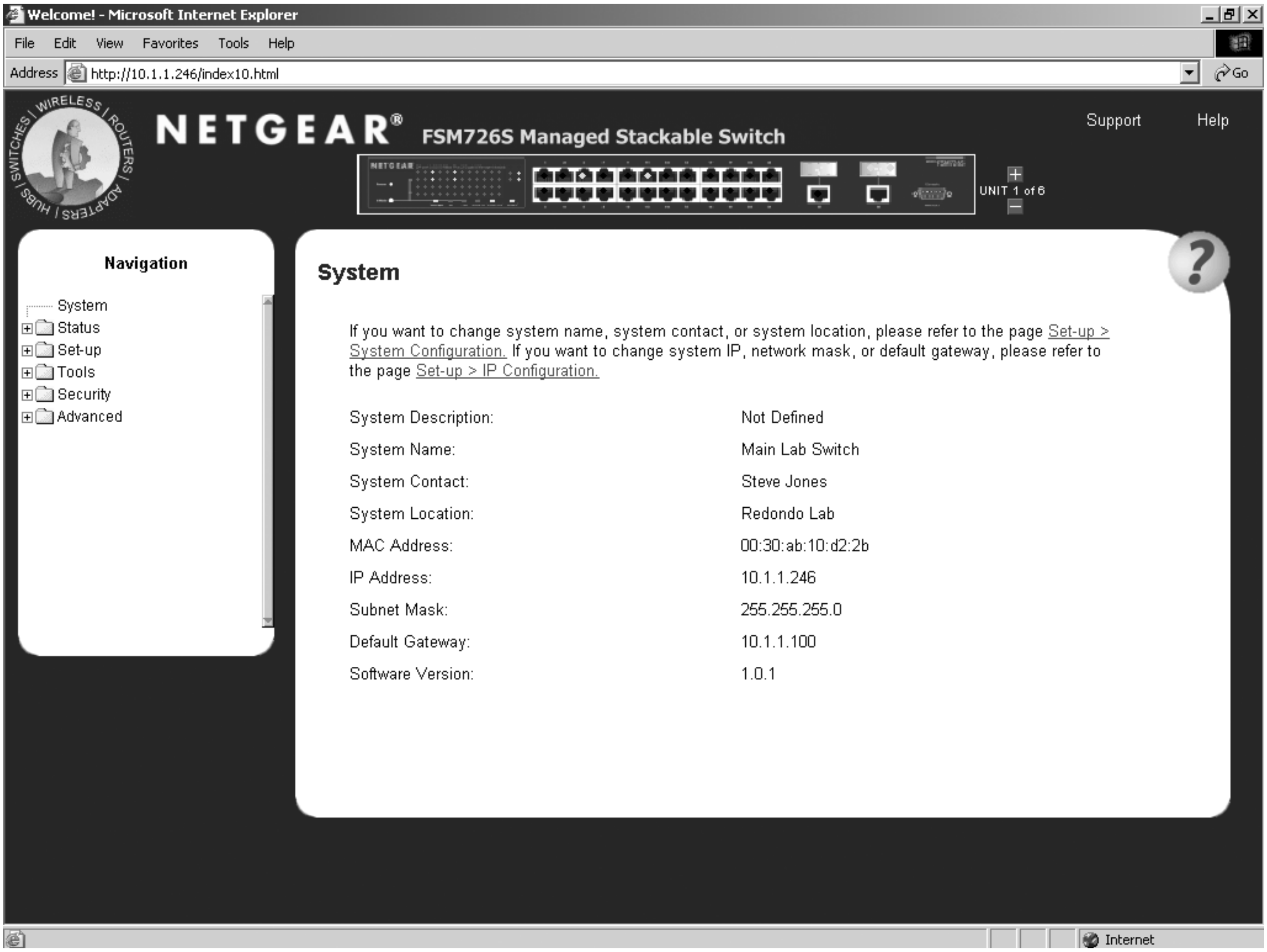
Reload:	Pulls that screen’s data from current values on the system
Apply:	Submits change request to system and refreshes screen data
Add:	Adds new entries to table information and refreshes screen data
Remove:	Removes selected entries from table and refreshes screen data
Reset:	Reset system, the action is equivalent to power off /on.
Restore:	Restore the system factory default value, except password and IP.
Query:	System will retrieve the useful information in database.

System

This is a welcome page, which displays system information, such as:

- System Description
- System Name
- System Contact
- System Location
- MAC Address
- IP Address
- Subnet Mask
- Default Gateway
- Software Version

These parameters are not editable from this screen. They can be modified in the Set Up> System Configuration page.



Welcome! - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://10.1.1.246/index10.html
Go
NETGEAR® FSM726S Managed Stackable Switch
Support
Help
UNIT 1 of 6
Navigation
System
Status
Set-up
Tools
Security
Advanced
Internet

System

If you want to change system name, system contact, or system location, please refer to the page Set-up > System Configuration. If you want to change system IP, network mask, or default gateway, please refer to the page Set-up > IP Configuration.

System Description:	Not Defined
System Name:	Main Lab Switch
System Contact:	Steve Jones
System Location:	Redondo Lab
MAC Address:	00:30:ab:10:d2:2b
IP Address:	10.1.1.246
Subnet Mask:	255.255.255.0
Default Gateway:	10.1.1.100
Software Version:	1.0.1

Figure 7-3: System

Status

The Status page contains 5 menus:

- Switch Statistics
- Port Statistics
- Port Settings
- MAC Address Table
- Error Chart

Status > Switch Statistics

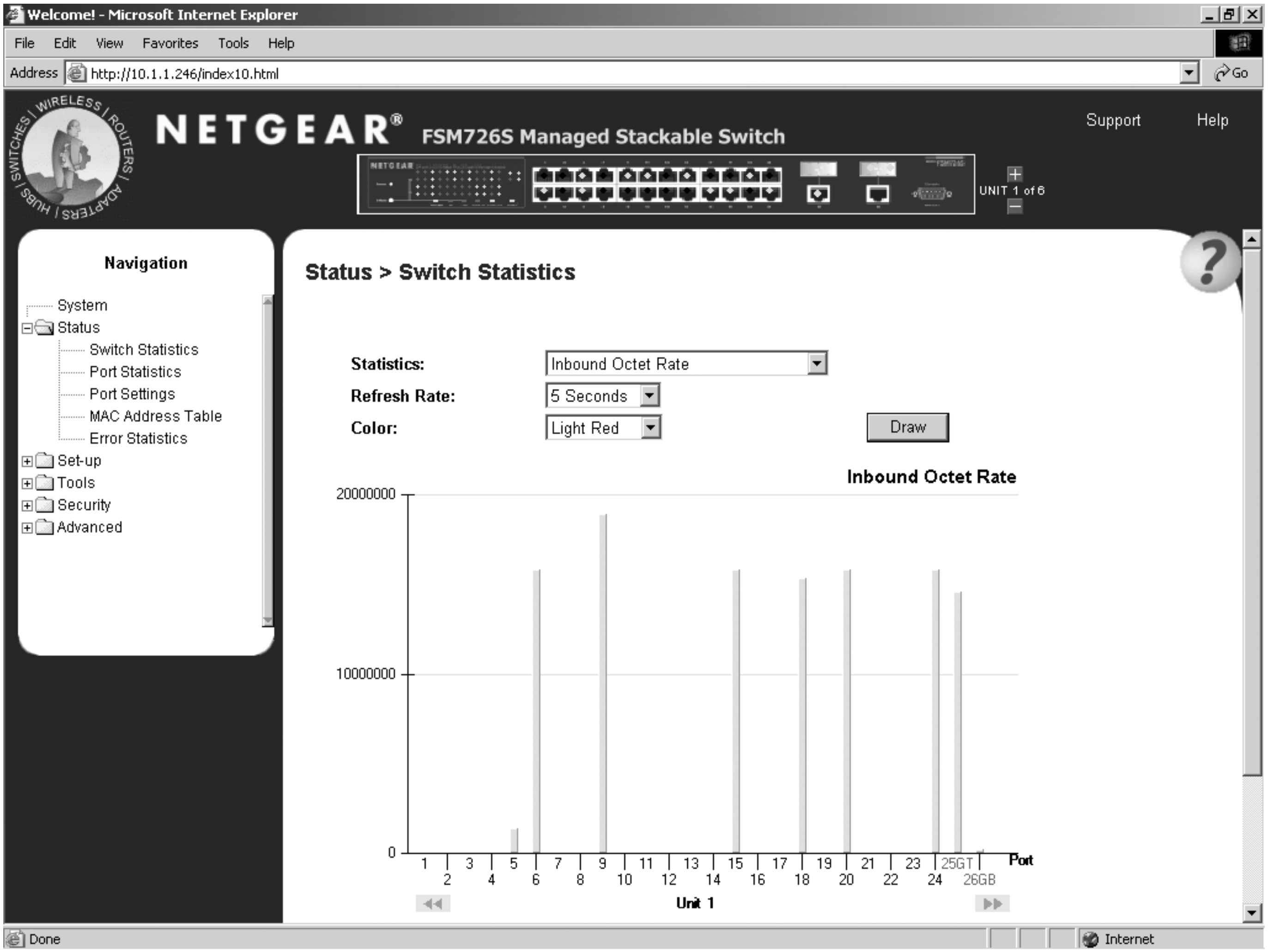
The Switch Statistics Chart allows you to compare one type of statistic across all the ports.

<u>Switch Statistics Chart</u>

- Statistics The type of system data to be monitored
- Refresh Rate The time interval between automatic refreshes (5, 10, 15, 30 seconds)
- Color The color setting for the chart

There are 24 kinds of Statistics that you can review on this screen:

Inbound Octet Rate: Received Byte per second.
Inbound Unicast Packet Rate: Received Unicast packet per second.
Inbound Non-unicast Packet rate: Received Non-unicast packet per second.
Inbound Discard Rate: Received and is discarded packet per second.
Inbound Error Rate: Received error packet per second.
Outbound Octet Rate: Transmitted byte per second.
Outbound Unicast Packet Rate: Transmitted unicast packet per second.
Outbound Non-unicast Packet rate: Transmitted non-unicast packet per second.
Outbound Discard Rate: Transmitted and is discarded packet per second.
Outbound Error Rate: Transmitted error packet per second.
Ethernet Undersize Packet Rate: Less than 64byte length packet per second.
Ethernet Oversize Packet Rate: More than 1518byte length packet per second
Inbound Octets: Received bytes
Inbound Unicast Packets: Received unicast packet
Inbound Non-unicast Packets: Received non-unicast packet
Inbound Discards: Received and is being discarded packet.
Inbound Errors: Received and is a error packet
Outbound Octets: Transmitted byte
Outbound Unicast Packets: Transmitted unicast packet
Outbound Non-unicast Packets: Transmitted non-unicast packet.
Outbound Discards: Transmitted and is being discarded packet
Outbound Errors: Transmitted and is an Error packet.
Ethernet Undersize Packets: Less than 64byte length packet
Ethernet Oversize Packets: more than 1518 byte length packet.



Status > Switch Statistics

Statistics: Inbound Octet Rate

Refresh Rate: 5 Seconds

Color: Light Red

Figure 7-4: Statistics: Switch Statistics

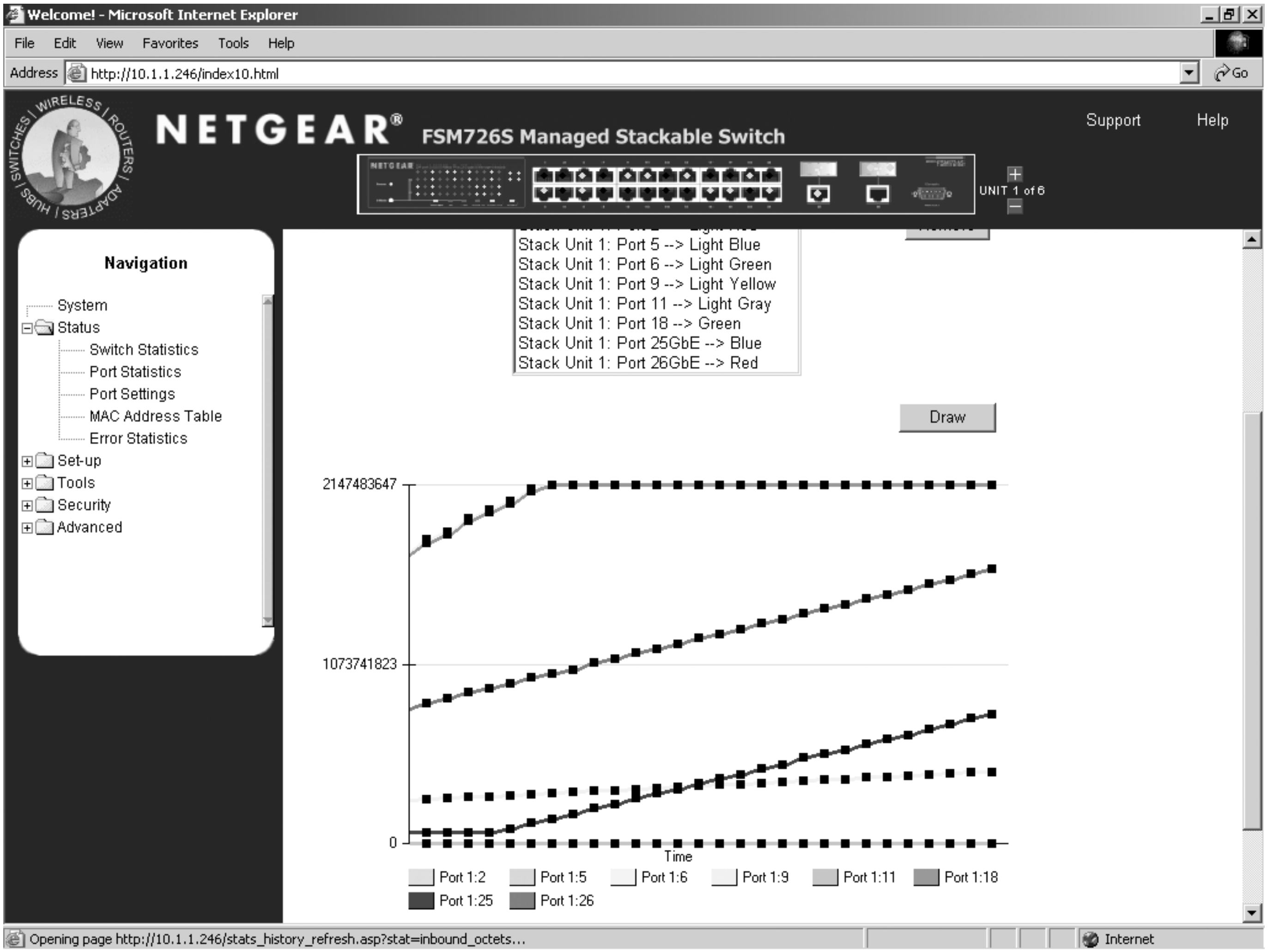
Status > Port Statistics

The Port Statistics Chart shows all the statistic types for one port over time.

- o Port — The port on which data will be monitored
- o Refresh Rate — The time interval between automatic refreshes
- o Color — The color setting for the data

There are 12 kinds of Port Statistics

Inbound Octets: Received bytes
Inbound Unicast Packets: Received unicast packet
Inbound Non-unicast Packets: Received non-unicast packet
Inbound Discards: Received and is being discarded packet.
Inbound Errors: Received and is a error packet
Outbound Octets: Transmitted byte
Outbound Unicast Packets: Transmitted unicast packet
Outbound Non-unicast Packets: Transmitted non-unicast packet.
Outbound Discards: Transmitted and is being discarded packet
Outbound Errors: Transmitted and is a Error packet.
Ethernet Undersize Packets: Less than 64byte length packet
Ethernet Oversize Packets: more than 1518 byte length packet.



Stack Unit 1: Port 5 --> Light Blue
Stack Unit 1: Port 6 --> Light Green
Stack Unit 1: Port 9 --> Light Yellow
Stack Unit 1: Port 11 --> Light Gray
Stack Unit 1: Port 18 --> Green
Stack Unit 1: Port 25GbE --> Blue
Stack Unit 1: Port 26GbE --> Red

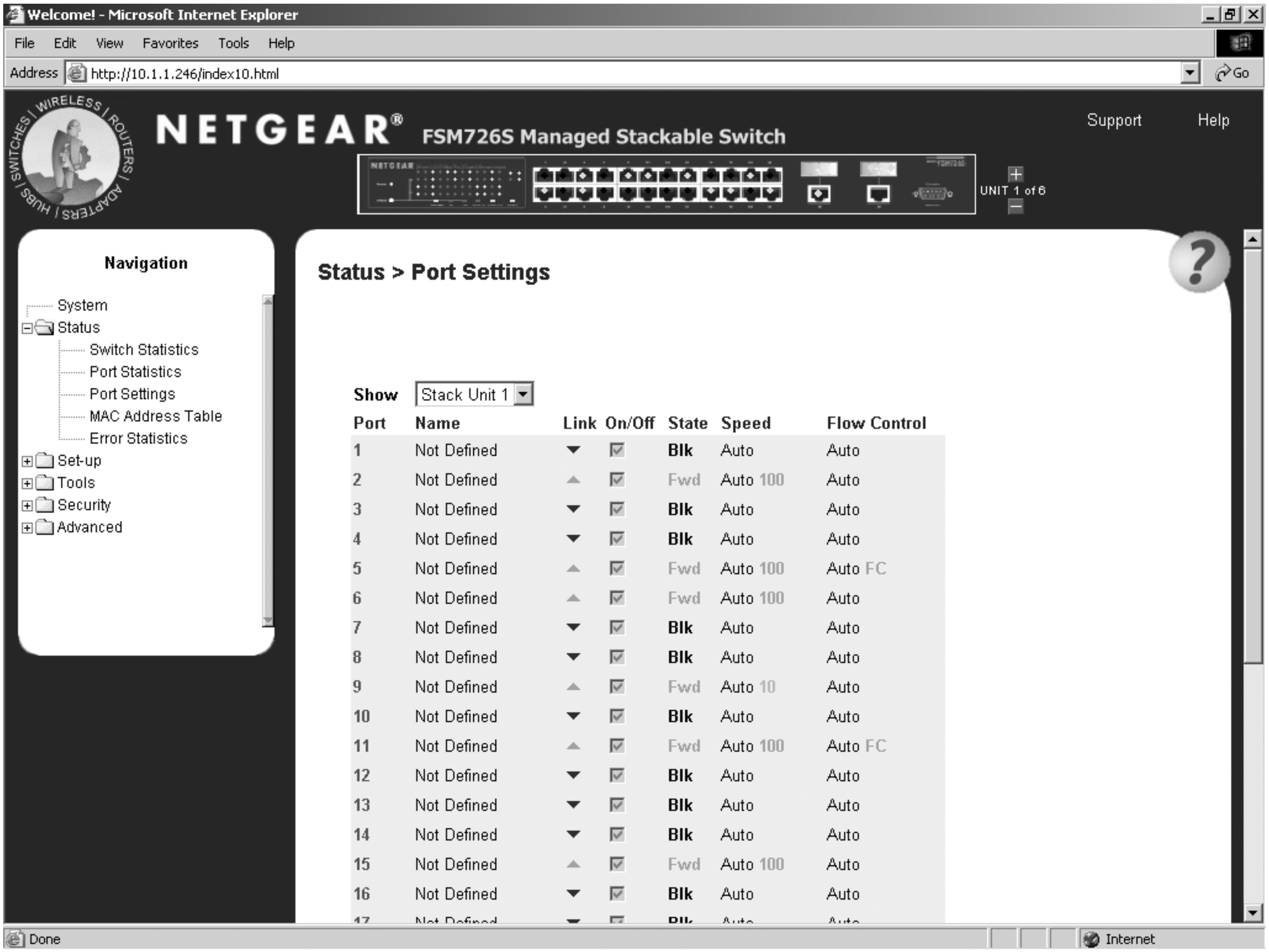
Opening page http://10.1.1.246/stats_history_refresh.asp?stat=inbound_octets...

Figure 7-5: Statistics: Port Statiscis

Status > Port Settings

This page displays the port settings. To configure the ports, go to the ‘Port Configuration’ under the ‘Set-up’ sub menu.

- Port Number: The port number on the switch
- Port Name: The name of the port. This is a user-defined label.
- Link Status: A green triangle pointing up indicates a valid link, while a red triangle pointing down indicates no link.
- On/Off: Indicates if the port is enabled or disabled by the Administrator.
- State: This refers to the Spanning Tree state of the port. Ports will be Blocking (Blk), Listening (Lis), Learning (Lrn), Forwarding (Fwd) or Disabled (Dis).
- Speed: Indicates the speed and duplex for the port. The possible entries are Auto-negotiation (Auto); 10 Mbps half duplex (10M Half); 10 Mbps full duplex (10M Full); 100 Mbps half duplex (100M Half); or 100 Mbps full duplex (100M Full).
- Flow Control: Indicates whether Flow Control support is set for automatic (Auto) or off (Disabled)



Status > Port Settings

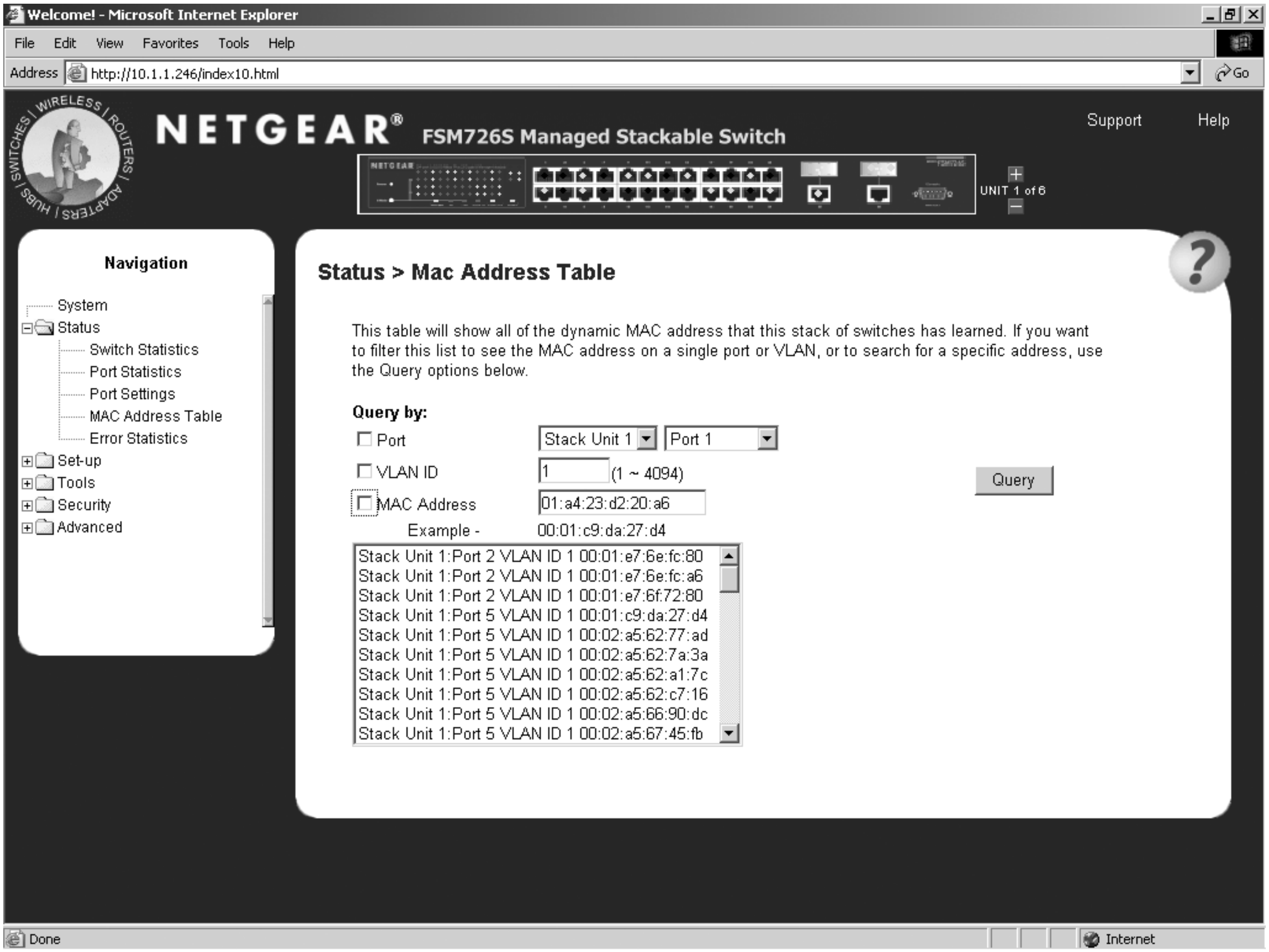
Show: Stack Unit 1

Port	Name	Link	On/Off	State	Speed	Flow Control
1	Not Defined	▼	☑	Blk	Auto	Auto
2	Not Defined	▲	☑	Fwd	Auto 100	Auto
3	Not Defined	▼	☑	Blk	Auto	Auto
4	Not Defined	▼	☑	Blk	Auto	Auto
5	Not Defined	▲	☑	Fwd	Auto 100	Auto FC
6	Not Defined	▲	☑	Fwd	Auto 100	Auto
7	Not Defined	▼	☑	Blk	Auto	Auto
8	Not Defined	▼	☑	Blk	Auto	Auto
9	Not Defined	▲	☑	Fwd	Auto 10	Auto
10	Not Defined	▼	☑	Blk	Auto	Auto
11	Not Defined	▲	☑	Fwd	Auto 100	Auto FC
12	Not Defined	▼	☑	Blk	Auto	Auto
13	Not Defined	▼	☑	Blk	Auto	Auto
14	Not Defined	▼	☑	Blk	Auto	Auto
15	Not Defined	▲	☑	Fwd	Auto 100	Auto
16	Not Defined	▼	☑	Blk	Auto	Auto
17	Not Defined	▼	☑	Blk	Auto	Auto

Figure 7-6: Port Configuration: Port Settings

Status > MAC Address Table

The MAC Address Table is a dynamic address lookup table allows you to view the dynamic MAC addresses that are currently in the address database. When addresses are in the database, the packets intended for those addresses are forwarded directly to those ports. You can filter the displayed addresses by port, VLAN, and/or MAC address by checking those fields.


Welcome! - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://10.1.1.246/index10.html
Go
WIRELESS / ROUTERS / ADAPTERS / HUBS / SWITCHES
NETGEAR® FSM726S Managed Stackable Switch
Support
Help
UNIT 1 of 6
Navigation
System
Status
Switch Statistics
Port Statistics
Port Settings
MAC Address Table
Error Statistics
Set-up
Tools
Security
Advanced
Query
Done
Internet

Status > Mac Address Table

This table will show all of the dynamic MAC address that this stack of switches has learned. If you want to filter this list to see the MAC address on a single port or VLAN, or to search for a specific address, use the Query options below.

Query by:

□ Port — Stack Unit 1 / Port 1

□ VLAN ID — 1 (1 ~ 4094)

□ MAC Address — 01:a4:23:d2:20:a6

Example - 00:01:c9:da:27:d4

```
Stack Unit 1:Port 2 VLAN ID 1 00:01:e7:6e:fc:80
Stack Unit 1:Port 2 VLAN ID 1 00:01:e7:6e:fc:a6
Stack Unit 1:Port 2 VLAN ID 1 00:01:e7:6f:72:80
Stack Unit 1:Port 5 VLAN ID 1 00:01:c9:da:27:d4
Stack Unit 1:Port 5 VLAN ID 1 00:02:a5:62:77:ad
Stack Unit 1:Port 5 VLAN ID 1 00:02:a5:62:7a:3a
Stack Unit 1:Port 5 VLAN ID 1 00:02:a5:62:a1:7c
Stack Unit 1:Port 5 VLAN ID 1 00:02:a5:62:c7:16
Stack Unit 1:Port 5 VLAN ID 1 00:02:a5:66:90:dc
Stack Unit 1:Port 5 VLAN ID 1 00:02:a5:67:45:fb
```

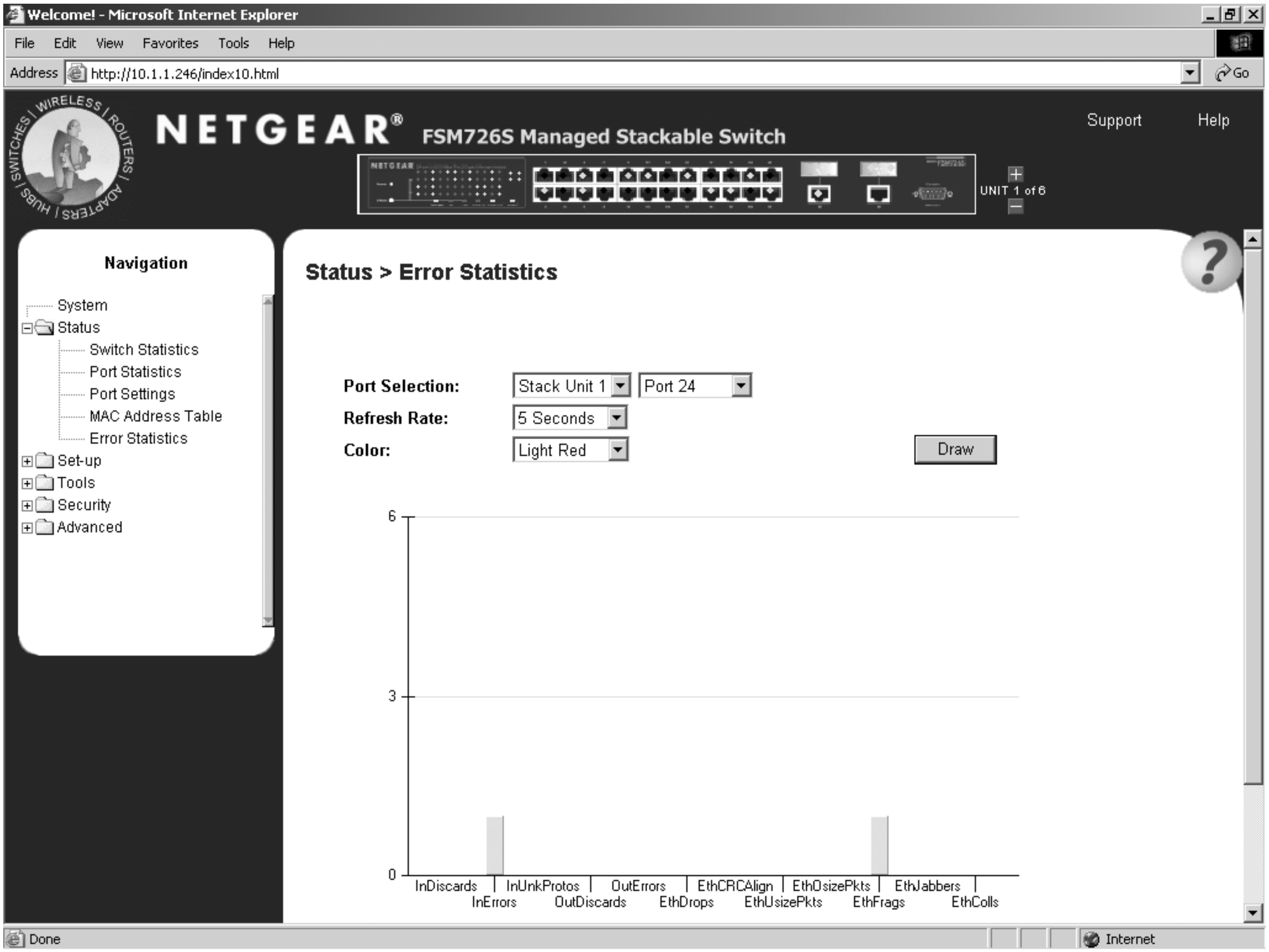
Figure 7-7: Status Manager: MAC Address Table

Status > Error Statistics

The Error Statistics Graph allows you to chart one type of statistic for any combination of ports. In the case of the Error Statistics Graph, the chart will present data across time so that fluctuations in time can be easily seen. All charts have a maximum ceiling of more than 2.1 billion (2,147,483,647). You can see the value of each bar or line in the chart by clicking on the bar. The following will outline the settings for each type of graph.

o	Statistics	The type of system errors to be monitored
o	Refresh Rate	The time interval between automatic refreshes (5,10,15, 30 seconds)
o	Port Selection	The port for data to be monitored

When all of the variables are set, click Draw.



Status > Error Statistics

Port Selection: Stack Unit 1 Port 24

Refresh Rate: 5 Seconds

Color: Light Red

Figure 7-8: Statistics: Error Statistics

Set-up

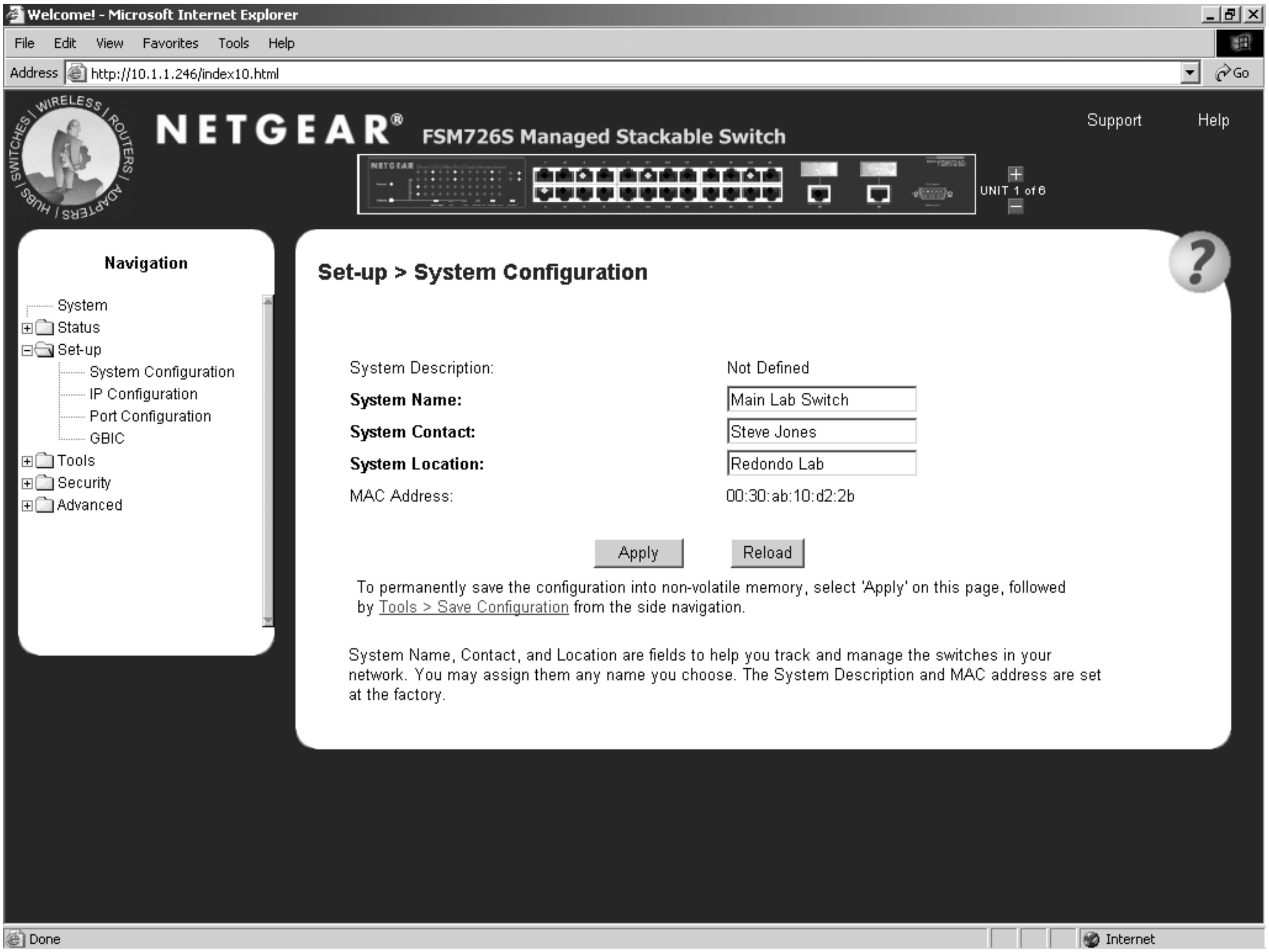
There are four kinds of configuration in the Setup page:

- System Configuration
- IP Configuration
- Port Configuration
- Gigabit Port Configuration (GBIC)

Set-up> System Configuration

This page will allow access to the system information parameters.

- Enter System Name, System Contact, System Location
- Click Apply to change the System Configuration
- Save Configuration to NVRAM and reset the system to implement the changes (Tools > Save Configuration)


Welcome! - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://10.1.1.246/index10.html
Go
NETGEAR® FSM726S Managed Stackable Switch
Support
Help
UNIT 1 of 6
Navigation
System
Status
Set-up
System Configuration
IP Configuration
Port Configuration
GBIC
Tools
Security
Advanced
Done
Internet

Set-up > System Configuration

System Description:	Not Defined
System Name:	Main Lab Switch
System Contact:	Steve Jones
System Location:	Redondo Lab
MAC Address:	00:30:ab:10:d2:2b

Apply Reload

To permanently save the configuration into non-volatile memory, select 'Apply' on this page, followed by Tools > Save Configuration from the side navigation.

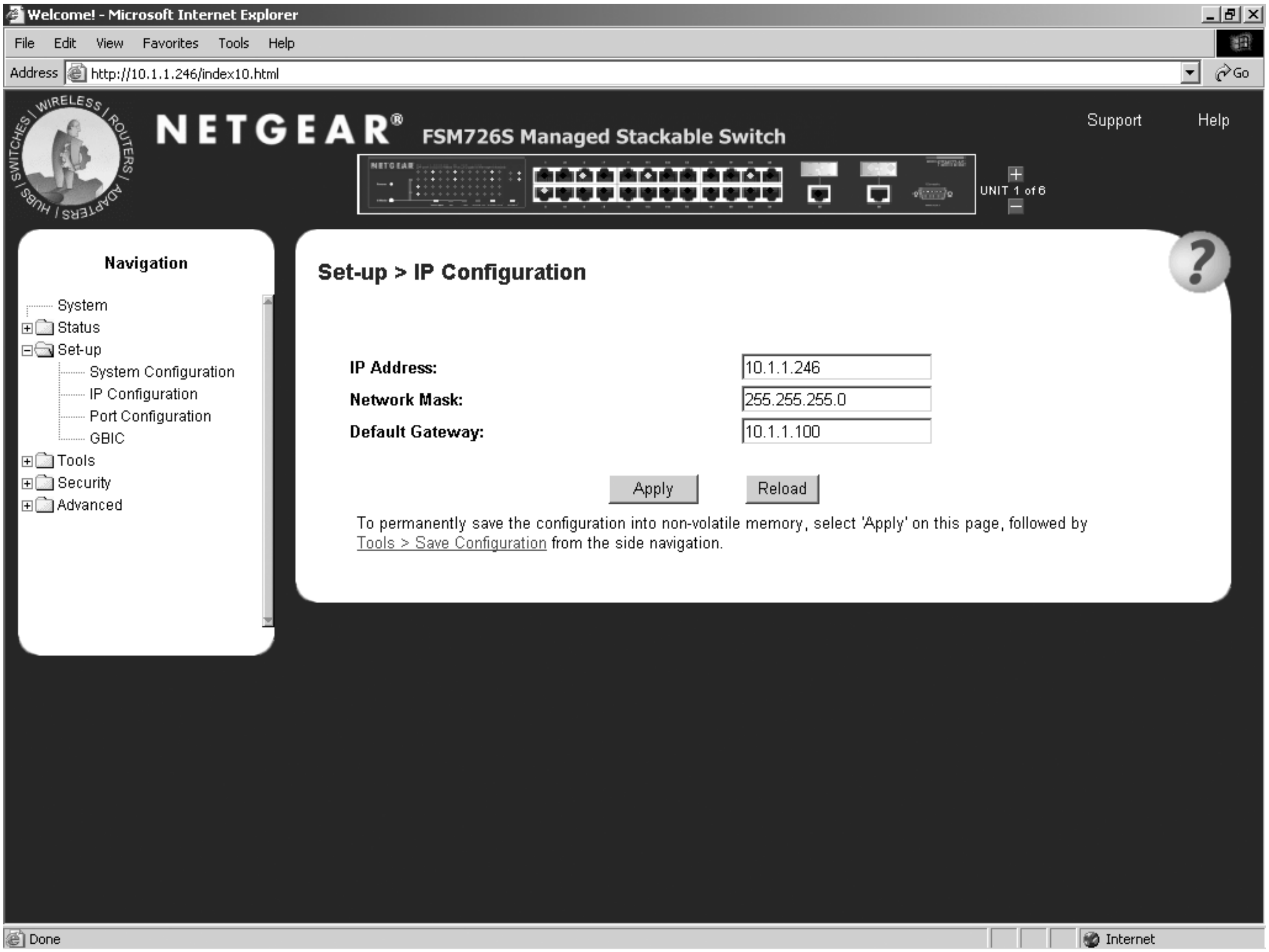
System Name, Contact, and Location are fields to help you track and manage the switches in your network. You may assign them any name you choose. The System Description and MAC address are set at the factory.

Figure 7-9: System Configuration

Set-up> IP Configuration

You can manage this switch over the network using its IP address, as set in this menu.
There are three tunable parameters to be set by the system administrator.

- Enter site-specific IP address, Gateway address and Net mask
- Click Apply to change the IP settings
- Save Configuration to NVRAM and reset the system to implement the changes (Tools > Save Configuration)



Set-up > IP Configuration

IP Address: 10.1.1.246
Network Mask: 255.255.255.0
Default Gateway: 10.1.1.100

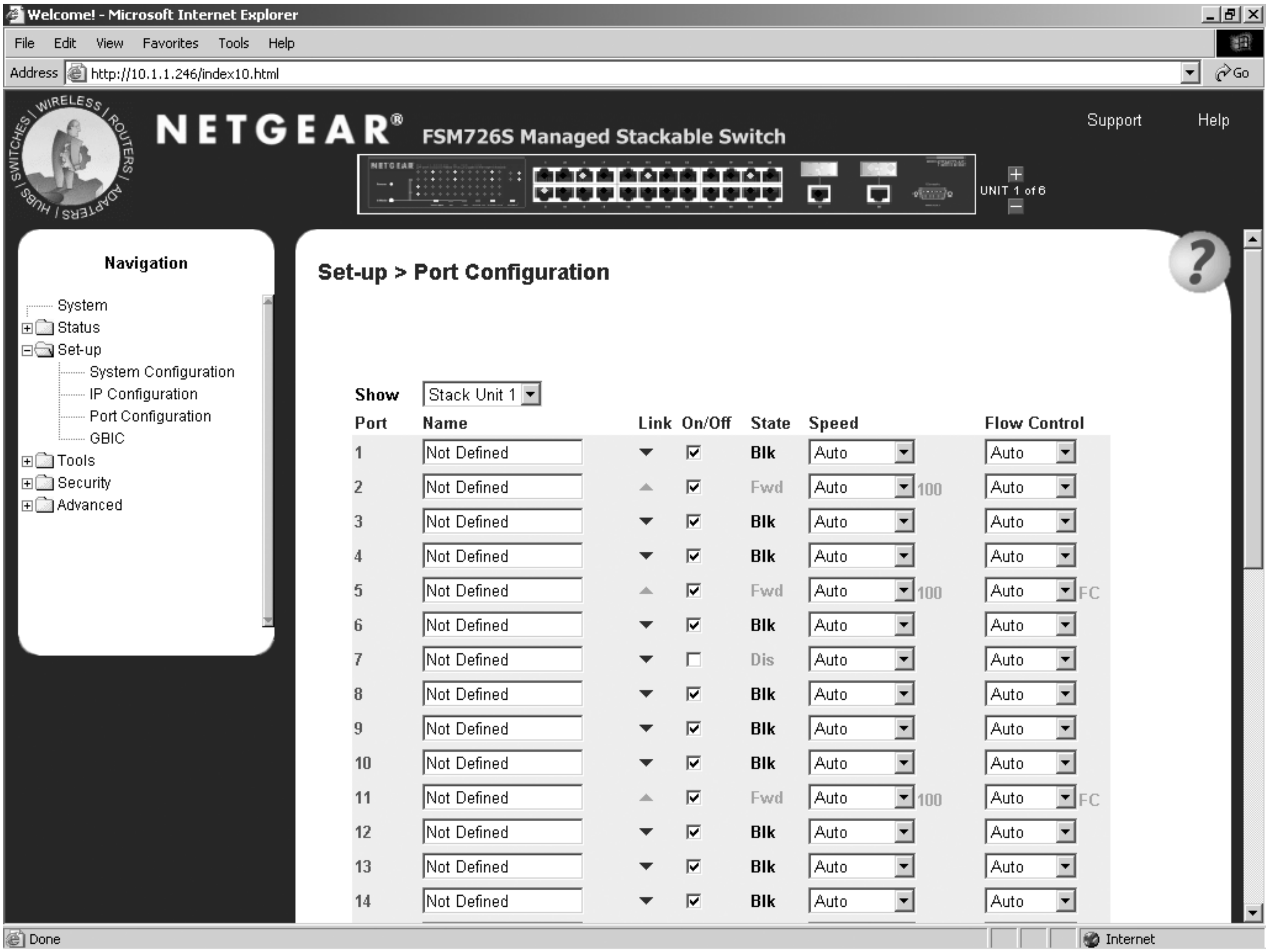
To permanently save the configuration into non-volatile memory, select 'Apply' on this page, followed by Tools > Save Configuration from the side navigation.

Figure 7-10: System Manager: IP Configuration

Set-up> Port Configuration

You can configure the status per port at 'Port Configuration' menu.

- Port Number: The port number on the switch
- Port Name: The name of the port. This is a user-defined label.
- Link Status: A green triangle pointing up indicates a valid link, while a red triangle pointing down indicates no link.
- On/Off: Indicates if the port is enabled or disabled by the Administrator.
- State: This refers to the Spanning Tree state of the port. Ports will be Blocking (Blk), Listening (Lis), Learning (Lrn), Forwarding (Fwd) or Disabled (Dis).
- Speed: Indicates the speed and duplex for the port. The possible entries are Auto-negotiation (Auto); 10 Mbps half duplex (10M Half); 10 Mbps full duplex (10M Full); 100 Mbps half duplex (100M Half); or 100 Mbps full duplex (100M Full).
- Flow Control: Indicates whether Flow Control support is set for automatic (Auto) or off (Disabled)


Welcome! - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://10.1.1.246/index10.html
Go
NETGEAR® FSM726S Managed Stackable Switch
Support
Help
UNIT 1 of 8
Navigation
System
Status
Set-up
System Configuration
IP Configuration
Port Configuration
GBIC
Tools
Security
Advanced
Done
Internet

Set-up > Port Configuration

Show Stack Unit 1

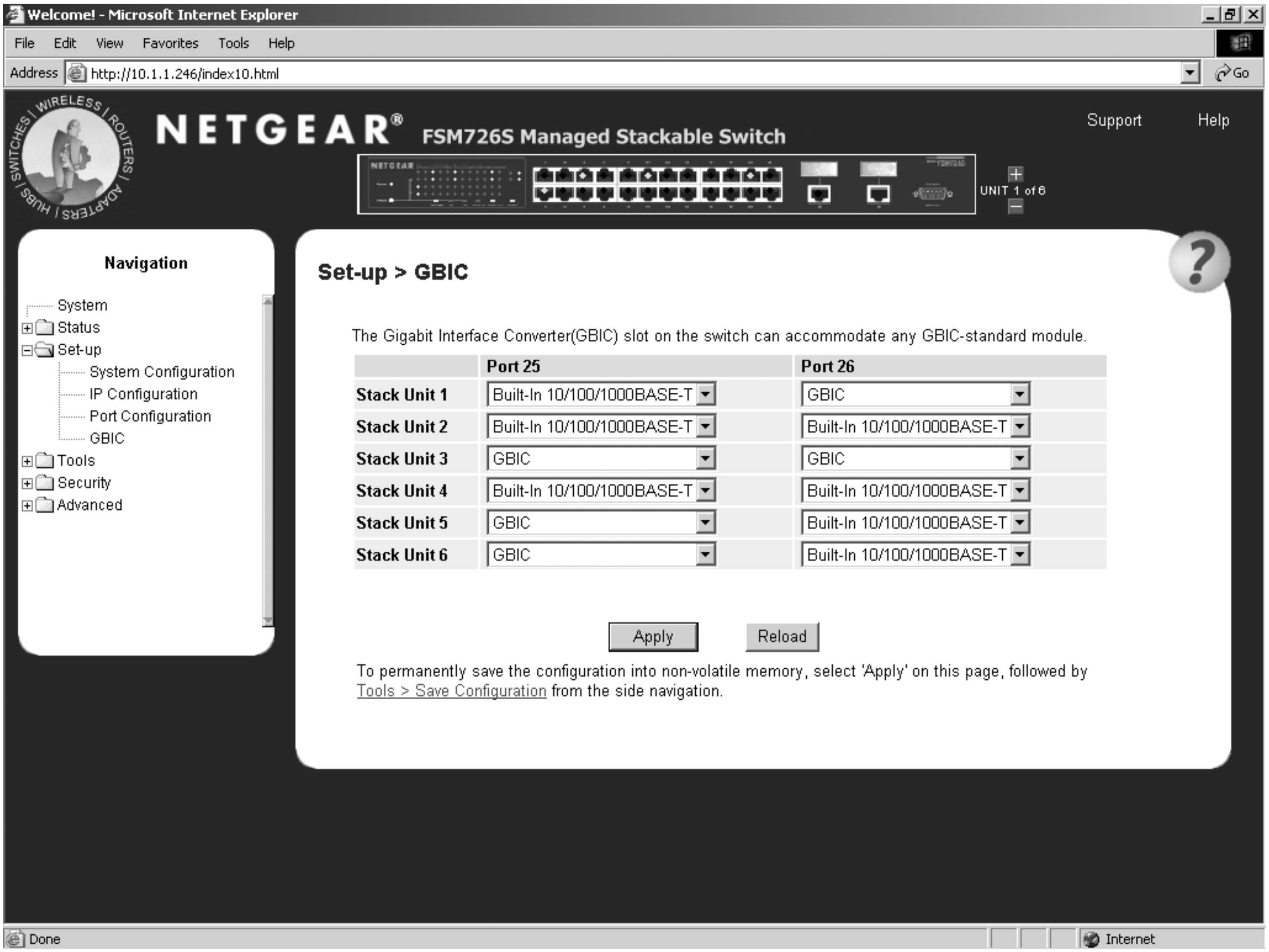
Port	Name	Link	On/Off	State	Speed	Flow Control
1	Not Defined	▼	☑	Blk	Auto	Auto
2	Not Defined	▲	☑	Fwd	Auto 100	Auto
3	Not Defined	▼	☑	Blk	Auto	Auto
4	Not Defined	▼	☑	Blk	Auto	Auto
5	Not Defined	▲	☑	Fwd	Auto 100	Auto FC
6	Not Defined	▼	☑	Blk	Auto	Auto
7	Not Defined	▼	□	Dis	Auto	Auto
8	Not Defined	▼	☑	Blk	Auto	Auto
9	Not Defined	▼	☑	Blk	Auto	Auto
10	Not Defined	▼	☑	Blk	Auto	Auto
11	Not Defined	▲	☑	Fwd	Auto 100	Auto FC
12	Not Defined	▼	☑	Blk	Auto	Auto
13	Not Defined	▼	☑	Blk	Auto	Auto
14	Not Defined	▼	☑	Blk	Auto	Auto

Figure 7-11: Setup: Port Configuration

Set-up> GBIC

This page allows the user to choose the port type of the gigabit ports. The default is copper (RJ-45). If the user chooses to use a GBIC, the setting on this page must be appropriately set.

Note: enabling the GBIC connector for a Gigabit Ethernet port disables the built-in 1000BASE-T port.


Welcome! - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://10.1.1.246/index10.html
Go
NETGEAR® FSM726S Managed Stackable Switch
Support
Help
UNIT 1 of 6
Navigation
System
Status
Set-up
System Configuration
IP Configuration
Port Configuration
GBIC
Tools
Security
Advanced
Done
Internet

Set-up > GBIC

The Gigabit Interface Converter(GBIC) slot on the switch can accommodate any GBIC-standard module.

	Port 25	Port 26
Stack Unit 1	Built-In 10/100/1000BASE-T	GBIC
Stack Unit 2	Built-In 10/100/1000BASE-T	Built-In 10/100/1000BASE-T
Stack Unit 3	GBIC	GBIC
Stack Unit 4	Built-In 10/100/1000BASE-T	Built-In 10/100/1000BASE-T
Stack Unit 5	GBIC	Built-In 10/100/1000BASE-T
Stack Unit 6	GBIC	Built-In 10/100/1000BASE-T

To permanently save the configuration into non-volatile memory, select 'Apply' on this page, followed by Tools > Save Configuration from the side navigation.

Figure 7-12: Setup: GBIC

Tools

The Tools page contains functions to maintain your switch. There is a firmware upgrade; the means to save current settings to non-volatile memory (NVRAM); as well as a software reset mechanism. The page has three sub-pages:

- Software Upgrade
- Save Configuration
- Device Reset

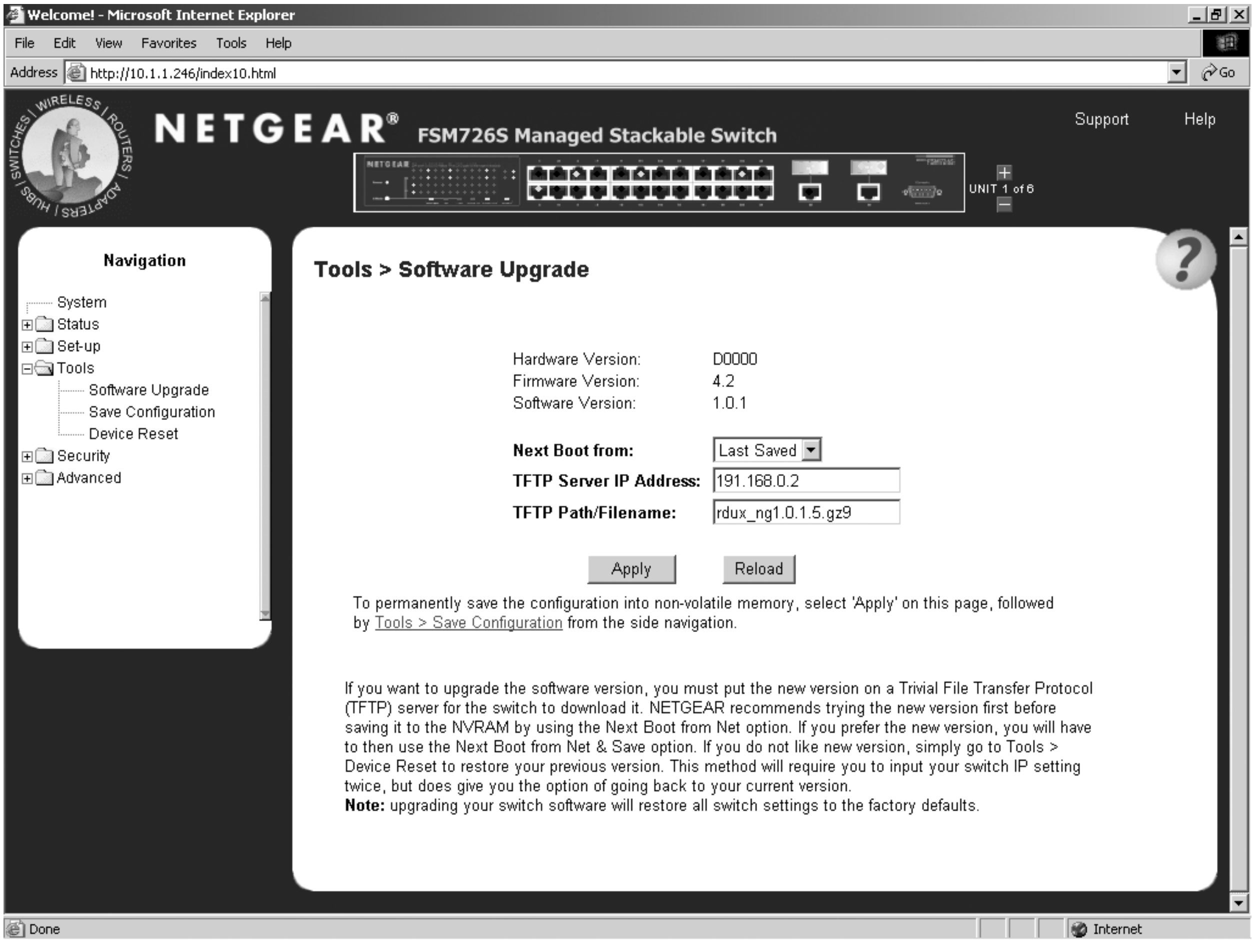
Tools> Software Upgrade

In the Software Upgrade screen, the system can be configured to download and boot from a new image from the network. Please refer to Chapter 5 when updating software.   Choose the method for the next system boot process: 'Net' will boot from the network, 'Net and Save' will boot from the network and permanently save the retrieved boot image in the switch, 'Last Saved' will boot from the boot image last saved in non-volatile memory in the switch. For booting from the network, supply the TFTP server IP address and boot image file name, then select 'Apply'.

Net option
This option allows the user to try out a new image before upgrading. It requires a TFTP filename and a server IP address to retrieve the specified image from the given IP address. The new image will not overwrite the one in non-volatile memory. (This is the default setting. See Figure 7-13)

Net & save option
This option requires the same setup as the Net option, i.e. TFTP server and a new image. However, it copies the image to non-volatile memory and then the system boots from non-volatile memory.

Last Saved option
The system will boot from non-volatile memory.   This option will automatically show up after the 'Net & save' option is selected and the unit is reset.


Welcome! - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://10.1.1.246/index10.html
Go
NETGEAR® FSM726S Managed Stackable Switch
Support
Help
UNIT 1 of 6
Navigation
System
Status
Set-up
Tools
Software Upgrade
Save Configuration
Device Reset
Security
Advanced
Done
Internet

Tools > Software Upgrade

Hardware Version: D0000
Firmware Version: 4.2
Software Version: 1.0.1

Next Boot from: Last Saved
TFTP Server IP Address: 191.168.0.2
TFTP Path/Filename: rdux_ng1.0.1.5.gz9

Apply Reload

To permanently save the configuration into non-volatile memory, select 'Apply' on this page, followed by Tools > Save Configuration from the side navigation.

If you want to upgrade the software version, you must put the new version on a Trivial File Transfer Protocol (TFTP) server for the switch to download it. NETGEAR recommends trying the new version first before saving it to the NVRAM by using the Next Boot from Net option. If you prefer the new version, you will have to then use the Next Boot from Net & Save option. If you do not like new version, simply go to Tools > Device Reset to restore your previous version. This method will require you to input your switch IP setting twice, but does give you the option of going back to your current version.
Note: upgrading your switch software will restore all switch settings to the factory defaults.

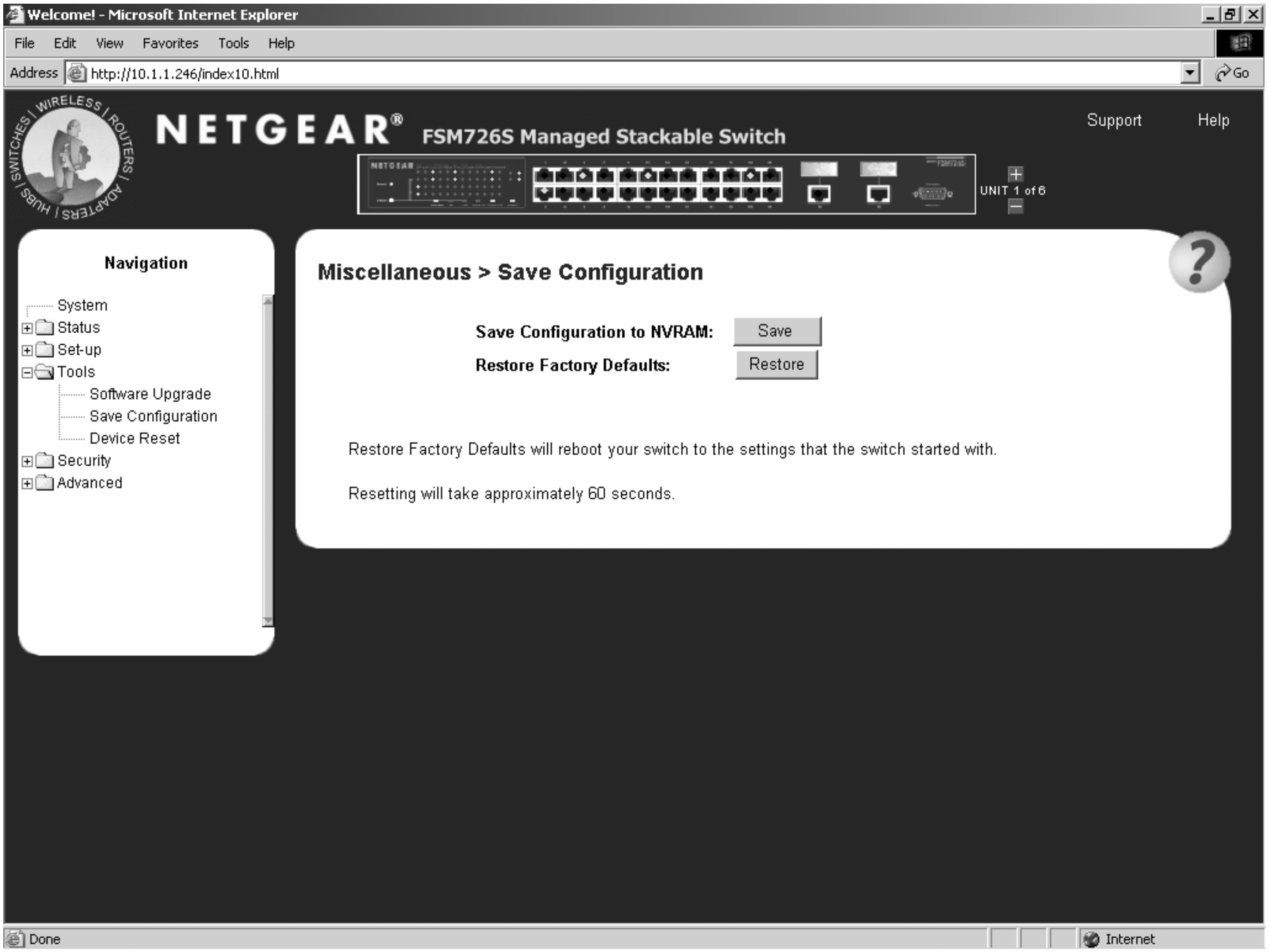
Figure 7-13: Software Upgrade

Tools> Save Configuration

After making any changes to the screens within the Web Interface, you can save the changed settings to NVRAM. If changes are not saved to NVRAM, then they will be lost during the next switch reset or reboot.

Restore the factory configuration by selecting 'Restore'.

Note: network IP settings (i.e. IP address, Gateway Address, Network Mask) will not be affected by the Restore command.


Welcome! - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://10.1.1.246/index10.html
Go
NETGEAR® FSM726S Managed Stackable Switch
Support
Help
UNIT 1 of 6
Navigation
System
Status
Set-up
Tools
Software Upgrade
Save Configuration
Device Reset
Security
Advanced
Save
Restore
Done
Internet

Miscellaneous > Save Configuration

Save Configuration to NVRAM: Save

Restore Factory Defaults: Restore

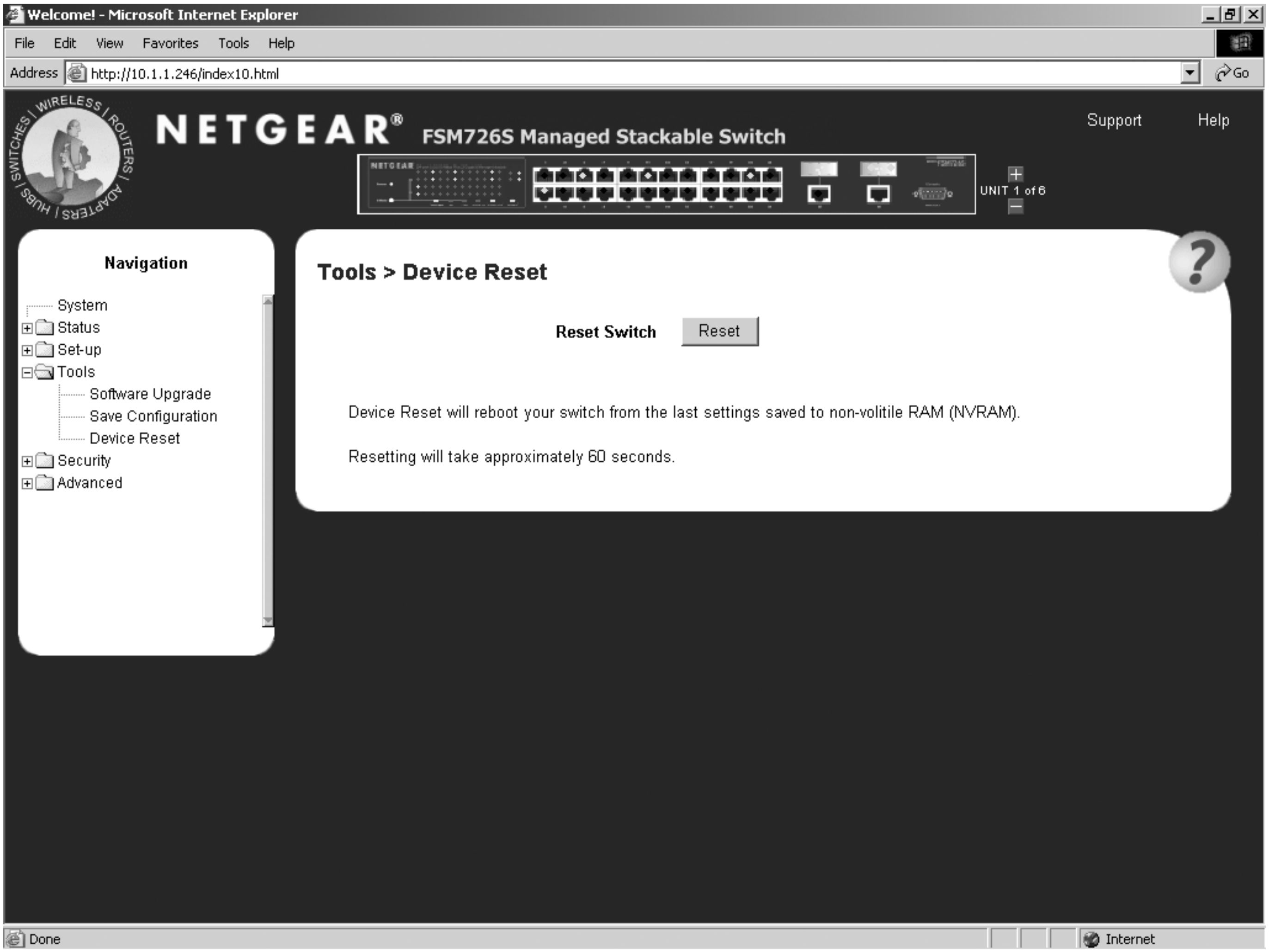
Restore Factory Defaults will reboot your switch to the settings that the switch started with.

Resetting will take approximately 60 seconds.

Figure 7-14: Save Configuration

Tools> Device Reset

In this screen the user can reset (power cycle) the switch. This is primarily used to upgrade the firmware or restore defaults. Reset the switch by selecting 'Reset'


Welcome! - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://10.1.1.246/index10.html
Go
NETGEAR® FSM726S Managed Stackable Switch
Support
Help
UNIT 1 of 6
Navigation
System
Status
Set-up
Tools
Software Upgrade
Save Configuration
Device Reset
Security
Advanced
Done
Internet

Tools > Device Reset

Reset Switch [Reset]

Device Reset will reboot your switch from the last settings saved to non-volitile RAM (NVRAM).

Resetting will take approximately 60 seconds.

Figure 7-15: Device Reset

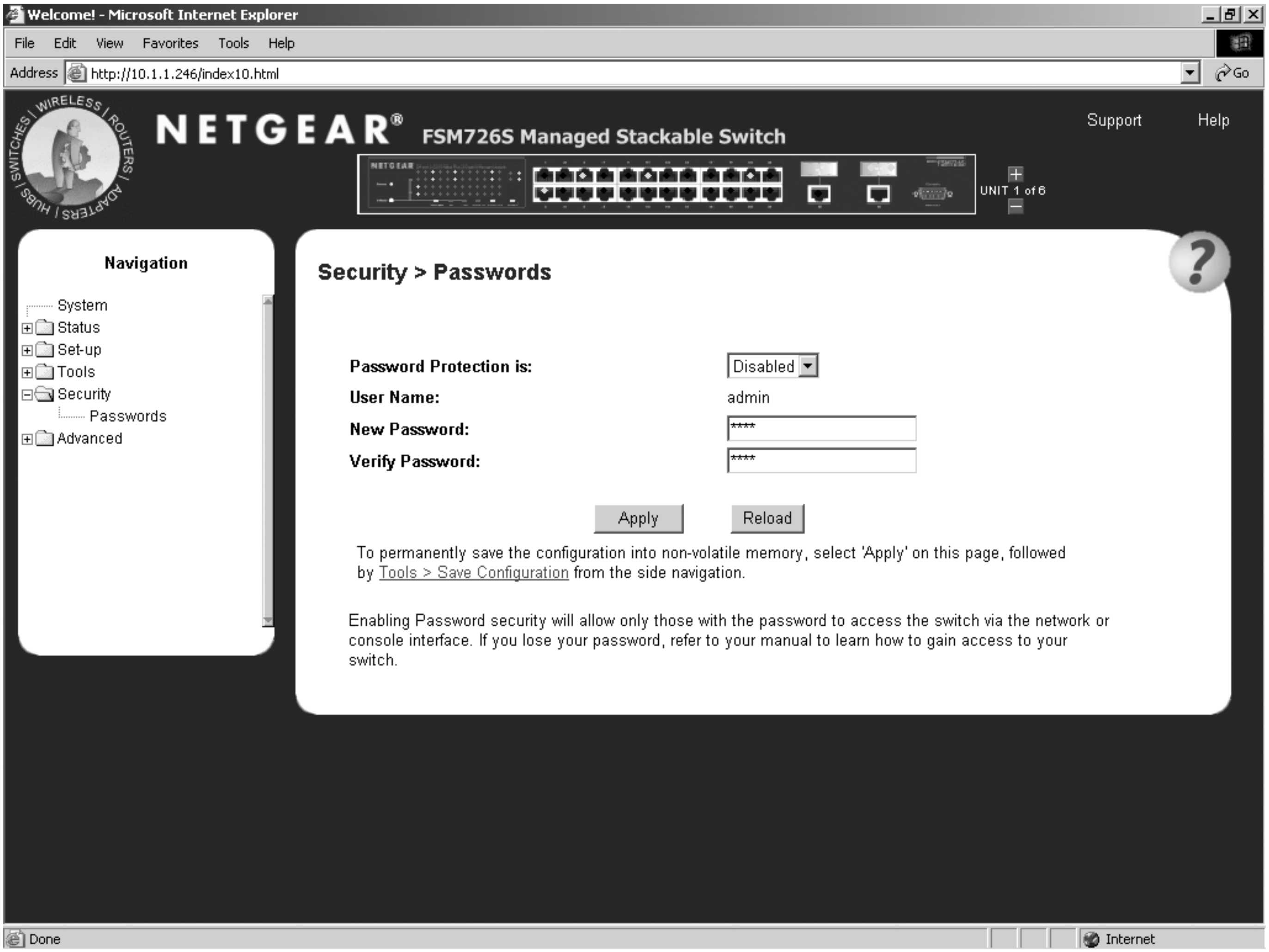
Security

Passwords

The password entered is encrypted on the screen and will display as a sequence of asterisks (*). The user name is 'admin' and cannot be changed. The user name and password are case sensitive.

- o Enable the password protection
- o Type the new administrator password in the New password field
- o Type the same password in the Verify field
- o Click Apply to activate the new password

Note: If you have enabled password protection without setting your own password, the default password is '1234'.


Welcome! - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://10.1.1.246/index10.html
Go
NETGEAR® FSM726S Managed Stackable Switch
Support
Help
UNIT 1 of 6
Navigation
System
Status
Set-up
Tools
Security
Passwords
Advanced
Apply
Reload
Done
Internet

Security > Passwords

Password Protection is: Disabled
User Name: admin
New Password: ****
Verify Password: ****

To permanently save the configuration into non-volatile memory, select 'Apply' on this page, followed by Tools > Save Configuration from the side navigation.

Enabling Password security will allow only those with the password to access the switch via the network or console interface. If you lose your password, refer to your manual to learn how to gain access to your switch.

Figure 7-16: System Manager: Password Admin

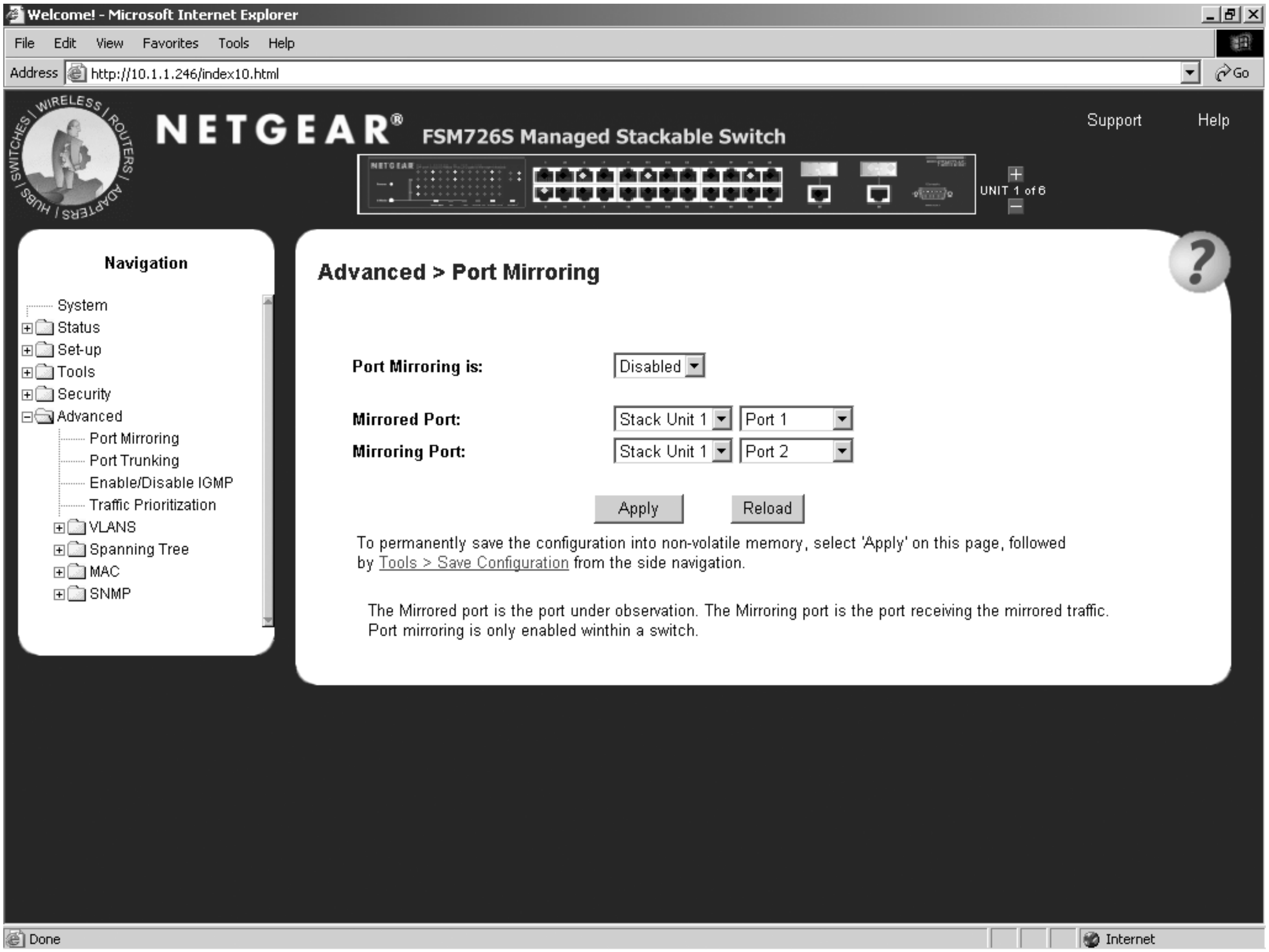
Advanced

The Advanced page allows professional users to operate more complicated features of the device, which include VLAN, Spanning Tree, Port Trunking, Multimedia support (IGMP), traffic prioritization, SNMP, and port mirroring. These features are powerful and can degrade or damage a network's performance if improperly used.

- Port Mirroring: Users can designate a port for monitoring traffic from one or more other ports or of a single VLAN configured on the switch. The switch monitors the network activity by copying all traffic from the specified monitoring sources to the designated monitoring port, to which a network analyzer can be attached.
- Port Trunking: a feature that allows multiple links between switches to work as one virtual link (aggregate link). Trunks can be defined for similar port types only. For example, a 10/100 port cannot form a Port Trunk with a gigabit port. For 10/100 ports, trunks can only be formed within the same bank. A bank is a set of eight ports. Up to four trunks can be operating at the same time. Toggle the ports to the correct trunk number to set up a trunk. After clicking Apply, the trunk will be enabled. Spanning Tree will treat trunked ports as a single virtual port.
- Multimedia Support (IGMP): The Internet Group Management Protocol (IGMP) is an Internet protocol that provides a way for network devices to report multicast group membership to adjacent routers.
- Traffic Prioritization (CoS): Class of Service (CoS), also referred to as Quality of Service (QoS), is a way of managing traffic in a network, by treating different types of traffic with different levels of service priority. Higher priority traffic gets faster treatment during times of switch congestion.
- VLANs: A Virtual Local Area Network (VLAN) is a means to electronically separate ports on the same switch from a single broadcast domain into separate broadcast domains. By using VLAN, users can group by logical function instead of physical location. There are 64VLAN supported on this switch.
- Spanning Tree Protocol (STP) ensures that only one path at a time is active between any two network nodes. There are maybe more than two physical path between any two nodes for redundant paths; STP ensures only one physical path is active and the others are blocked. STP will prevent an inadvertent loop in a network, which can disable your network due to a "Broadcast storm", the result of a broadcast message traveling through the loop again and again.
- MAC: MAC address table management

Advanced > Port Mirroring

Port mirroring is a feature to help in the debugging of a network. This web interface page allows the enabling or disabling of port mirroring and the setting of source and monitor ports. The monitor port will show a copy of every packet that arrives or leaves the source port.



Advanced > Port Mirroring

Port Mirroring is: Disabled

Mirrored Port: Stack Unit 1 Port 1

Mirroring Port: Stack Unit 1 Port 2

Apply Reload

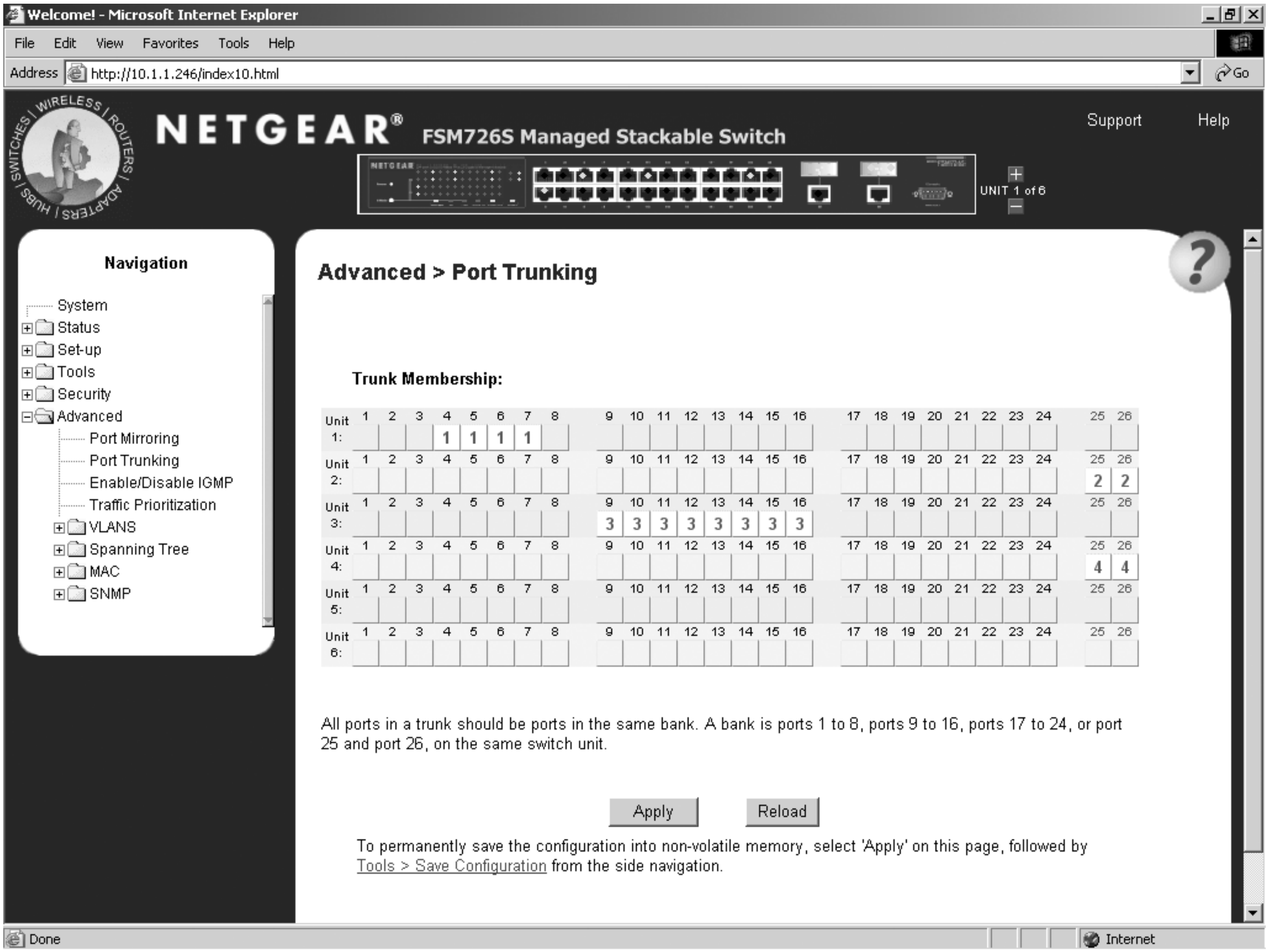
To permanently save the configuration into non-volatile memory, select 'Apply' on this page, followed by Tools > Save Configuration from the side navigation.

The Mirrored port is the port under observation. The Mirroring port is the port receiving the mirrored traffic. Port mirroring is only enabled winthin a switch.

Figure 7-17: Port Mirroring

Advanced > Port Trunking

Port Trunking is a feature that allows multiple links between switches to work as one virtual link (aggregate link). Trunks can be defined for similar port types only. For example, a 10/100 port cannot form a Port Trunk with a gigabit port. For 10/100 ports, trunks can only be formed within the same bank. . A bank is ports 1 to 8, ports 9 to 16, ports 17 to 24, or port 25 and port 26, on the same switch unit. Up to four trunks can be enabled at the same time within a stack. To set up a trunk, use the space bar to select the ports that will participate in the trunk. Spanning Tree will treat trunked ports as a single virtual port.



Advanced > Port Trunking

Trunk Membership:

Unit	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Unit 1:				1	1	1	1																			
Unit 2:																									2	2
Unit 3:									3	3	3	3	3	3	3	3										
Unit 4:																									4	4
Unit 5:																										
Unit 6:																										

All ports in a trunk should be ports in the same bank. A bank is ports 1 to 8, ports 9 to 16, ports 17 to 24, or port 25 and port 26, on the same switch unit.

To permanently save the configuration into non-volatile memory, select 'Apply' on this page, followed by Tools > Save Configuration from the side navigation.

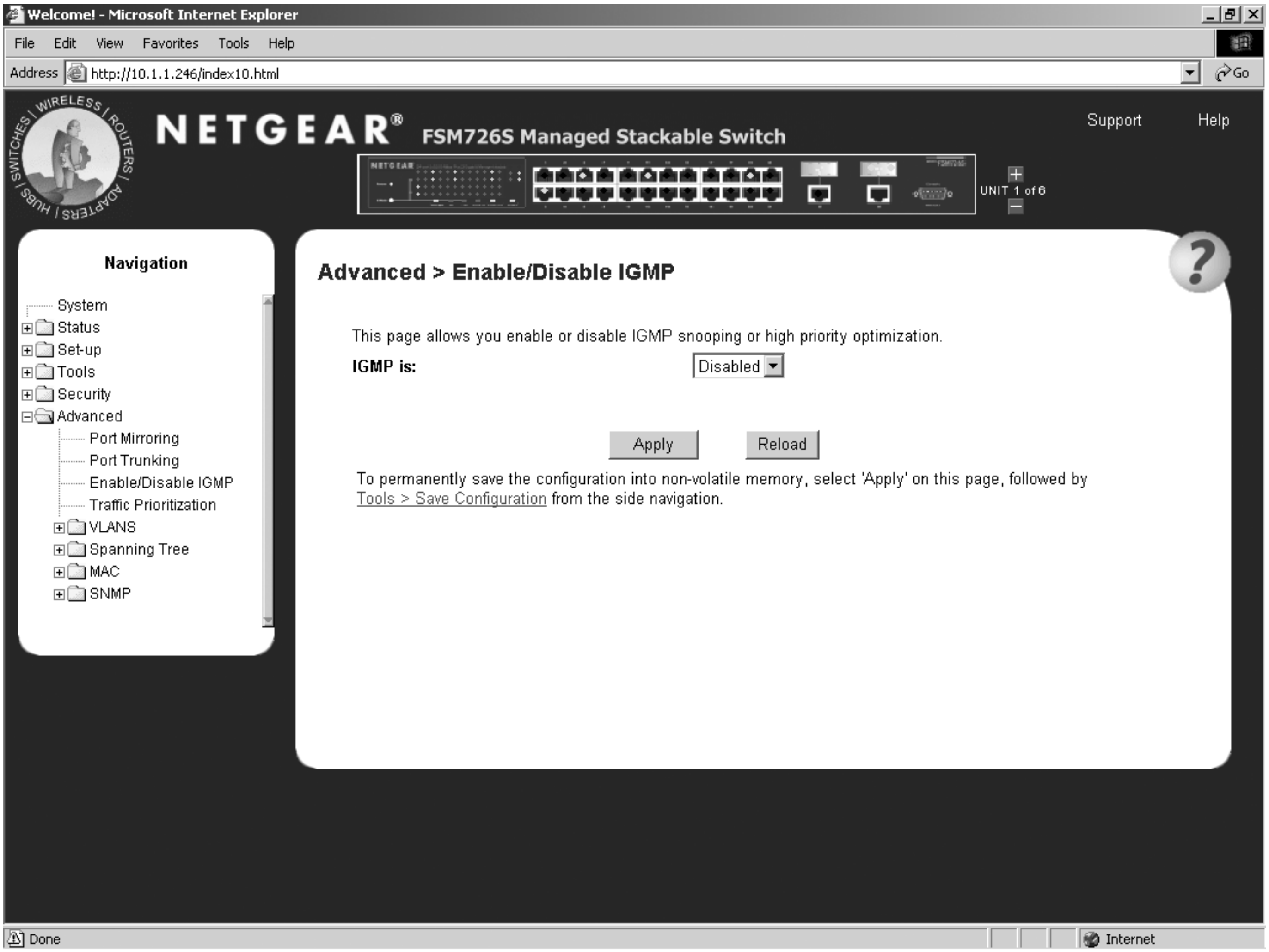
Figure 7-18: Port Trunking

Advanced > Enable/Disable IGMP

In networks where multimedia applications generate multicast traffic, IGMP can greatly reduce unnecessary bandwidth usage by limiting traffic forwarding that is otherwise broadcast to the whole network. Enabling IGMP will allow individual ports to detect IGMP queries, report packets, and manage IP multicast traffic through the switch.

IGMP

- o Enable The system will detect IGMP queries, report packets, and manage IP multicast traffic through the switch
- o Disable The switch will forward traffic disregarding any IGMP requests.



Advanced > Enable/Disable IGMP

This page allows you enable or disable IGMP snooping or high priority optimization.

IGMP is: Disabled

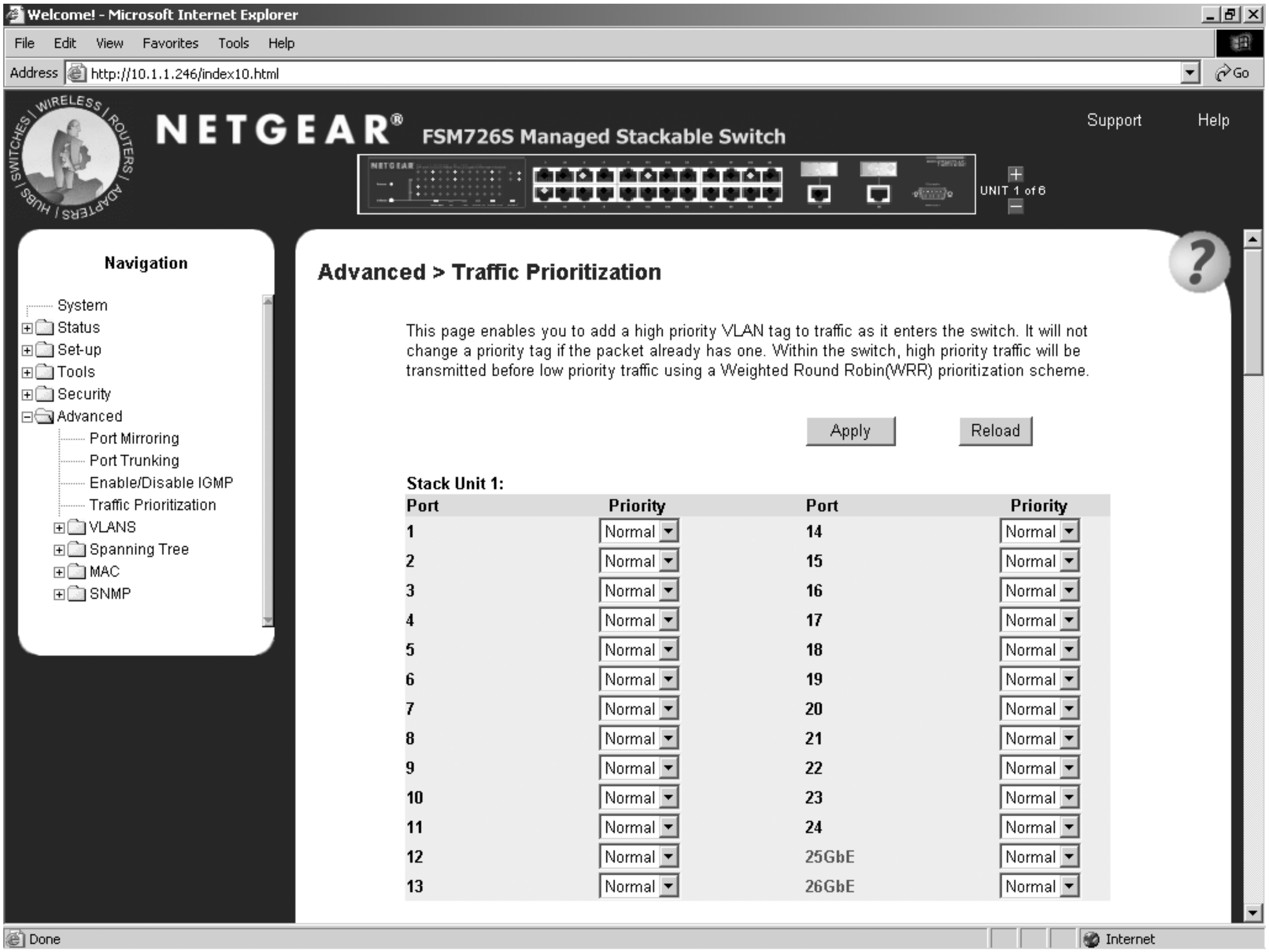
Apply Reload

To permanently save the configuration into non-volatile memory, select 'Apply' on this page, followed by Tools > Save Configuration from the side navigation.

Figure 7-19: IGMP

Advanced > Traffic Prioritization

Port Priority allows the user to specify which ports have greater precedence in situations where traffic may be buffered in the switch due to congestion. The ports with a setting of 'high' will transmit their packets before those with a 'normal' setting. The settings on this page only affect ingress packets that are not already tagged for priority. To raise the priority of a given port, switch the port's setting from 'normal' to 'high'. The default and normal setting for a port is 'normal'.



Advanced > Traffic Prioritization

This page enables you to add a high priority VLAN tag to traffic as it enters the switch. It will not change a priority tag if the packet already has one. Within the switch, high priority traffic will be transmitted before low priority traffic using a Weighted Round Robin(WRR) prioritization scheme.

Stack Unit 1:

Port	Priority	Port	Priority
1	Normal	14	Normal
2	Normal	15	Normal
3	Normal	16	Normal
4	Normal	17	Normal
5	Normal	18	Normal
6	Normal	19	Normal
7	Normal	20	Normal
8	Normal	21	Normal
9	Normal	22	Normal
10	Normal	23	Normal
11	Normal	24	Normal
12	Normal	25GbE	Normal
13	Normal	26GbE	Normal

Figure 7-20: Traffic Priortization Settings

Advanced> VLAN

VLANs: A Virtual Local Area Network (VLAN) is a means to electronically separate ports on the same switch from a single broadcast domain into separate broadcast domains. By using VLAN, users can group by logical function instead of physical location. There are 64VLAN supported on this switch. This switch supports static, port-based VLANs.

The VLAN tagging option is a standard set by the IEEE to facilitate the spanning of VLANs across multiple switches (Reference: Appendix C and IEEE Std 802.1Q-1998 Virtual Bridged Local Area Networks).

From this menu, you can create a new VLAN, add new ports to an existing VLAN, remove ports from an existing VLAN or, delete a VLAN.

Create a new VLAN Group

- Under the ‘Show VLAN’ drop down menu, select ‘Add a new VLAN’.
- Enter the VLAN Id and name in the provided fields.
- Add VLAN members if so desired. (See below).
- Click Apply.

Delete a VLAN Group

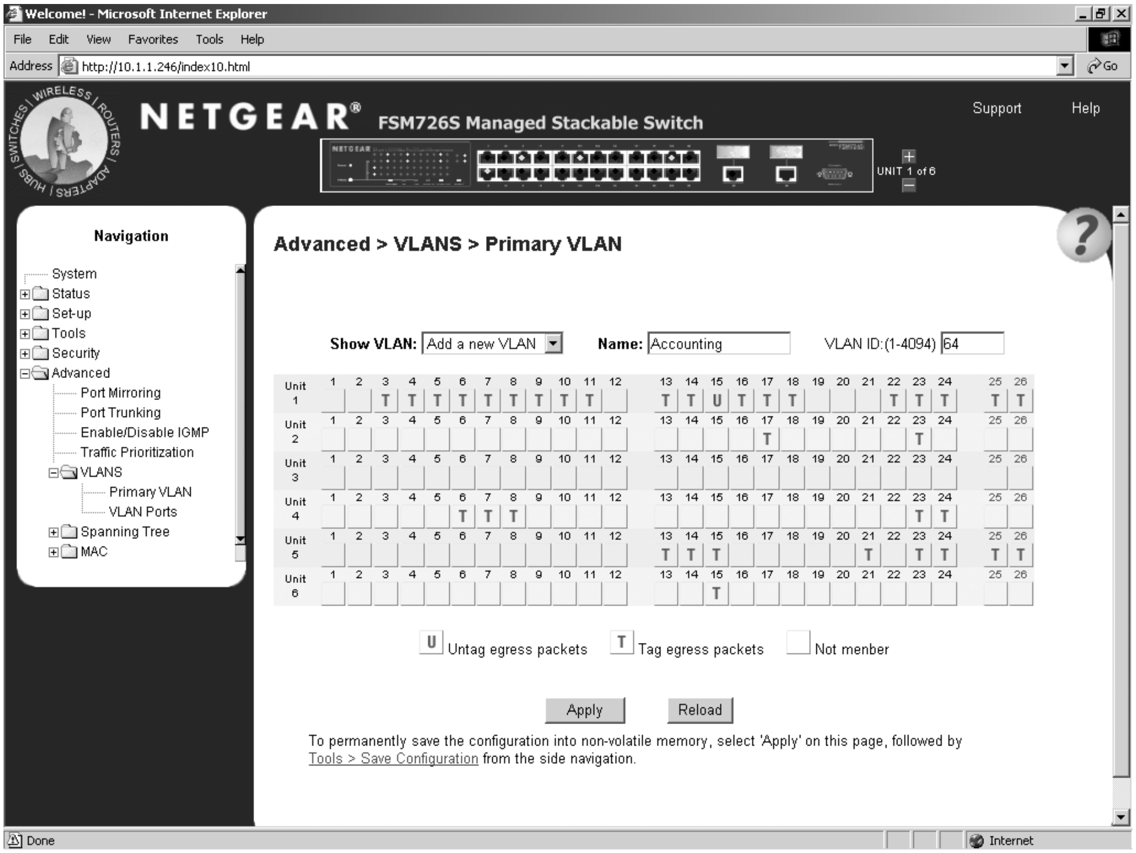
- Check the Remove VLAN box for the VLAN you want to remove.
- Click Apply.

Add a port to a VLAN Group

- Under the ‘Show VLAN’ drop down menu, select the VLAN you want to edit.
- Click the box below the port number on the line of the VLAN so that a ‘T’ (tagged) or ‘U’ (untagged) appears.
- Click Apply.

Remove a port from a VLAN Group

- Click the box again until a blank box appears. This will remove VLAN membership from the port.
- Click Apply.



Advanced > VLANS > Primary VLAN

Show VLAN: Add a new VLAN ▾ **Name:** Accounting VLAN ID:(1-4094) 64

Unit	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Unit 1			T	T	T	T	T	T	T	T	T		T	T	U	T	T	T				T	T	T	T	T
Unit 2																	T						T			
Unit 3																										
Unit 4						T	T	T															T	T		
Unit 5													T	T	T						T		T	T	T	T
Unit 6															T											

U Untag egress packets T Tag egress packets □ Not menber

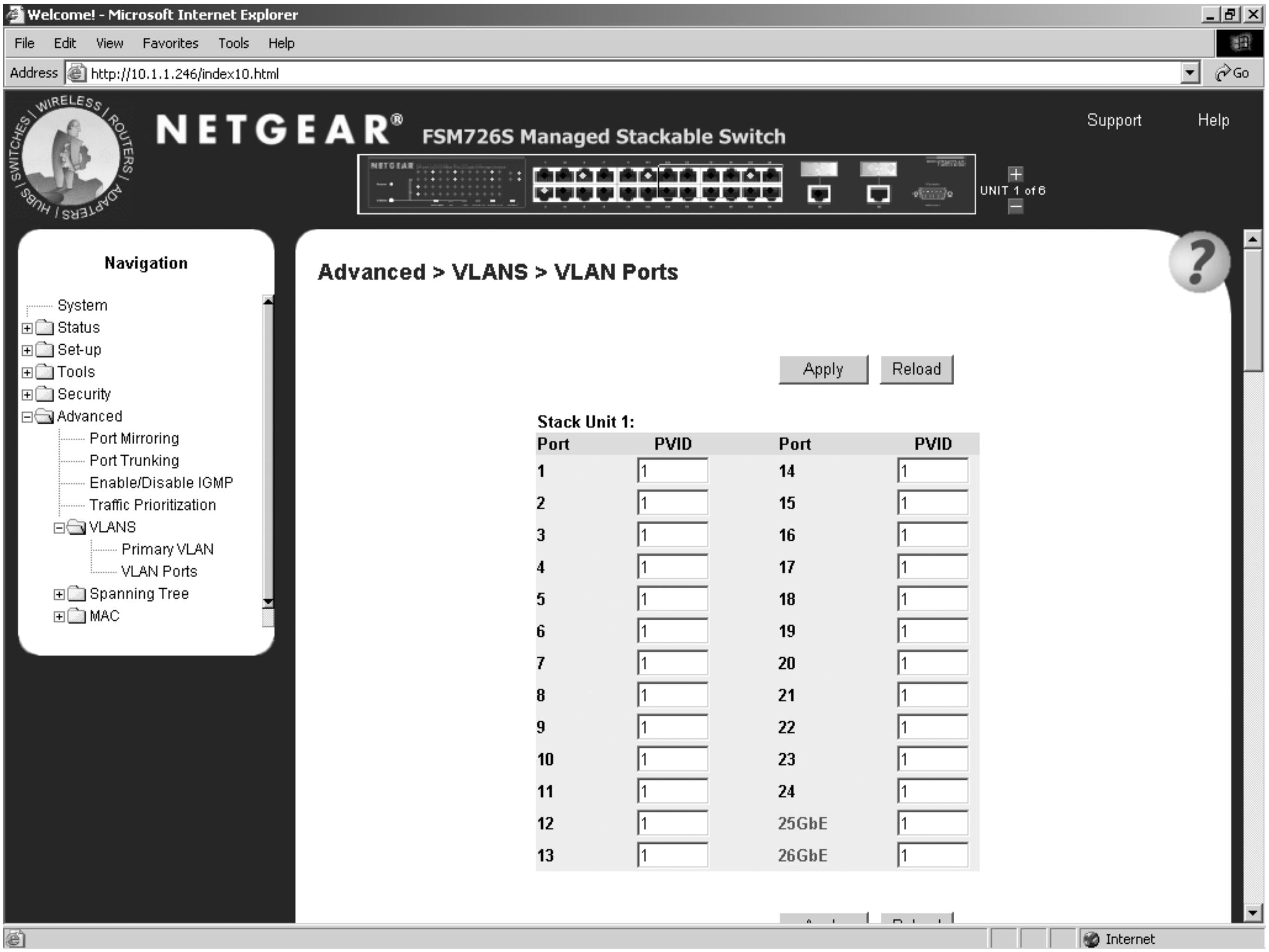
Apply Reload

To permanently save the configuration into non-volatile memory, select 'Apply' on this page, followed by Tools > Save Configuration from the side navigation.

Figure 7-21: VLANS: VLAN’s and Primary VLAN

Advanced> VLAN> VLAN Port

All untagged packets entering the switch will by default be tagged as specified by the port's Primary VLAN Identification (PVID). This screen allows you to specify the PVID for each port.



Advanced > VLANS > VLAN Ports

Stack Unit 1:

Port	PVID	Port	PVID
1	1	14	1
2	1	15	1
3	1	16	1
4	1	17	1
5	1	18	1
6	1	19	1
7	1	20	1
8	1	21	1
9	1	22	1
10	1	23	1
11	1	24	1
12	1	25GbE	1
13	1	26GbE	1

Figure 7-22: VLAN: VLAN Port Settings

Advanced> Spanning Tree

Spanning Tree Protocol (STP) ensures that only one path at a time is active between any two network nodes. There are maybe more than two physical path between any two nodes for redundant paths; STP ensures only one physical path is active and the others are blocked. STP will prevent an inadvertent loop in a network, which can disable your network due to a “Broadcast storm”, the result of a broadcast message traveling through the loop again and again.

There are two sub-page of Spanning Tree configuration:

- Bridge Settings
- Port Settings

Advanced> Spanning Tree > Bridge Settings

The following information is presented on the this page:

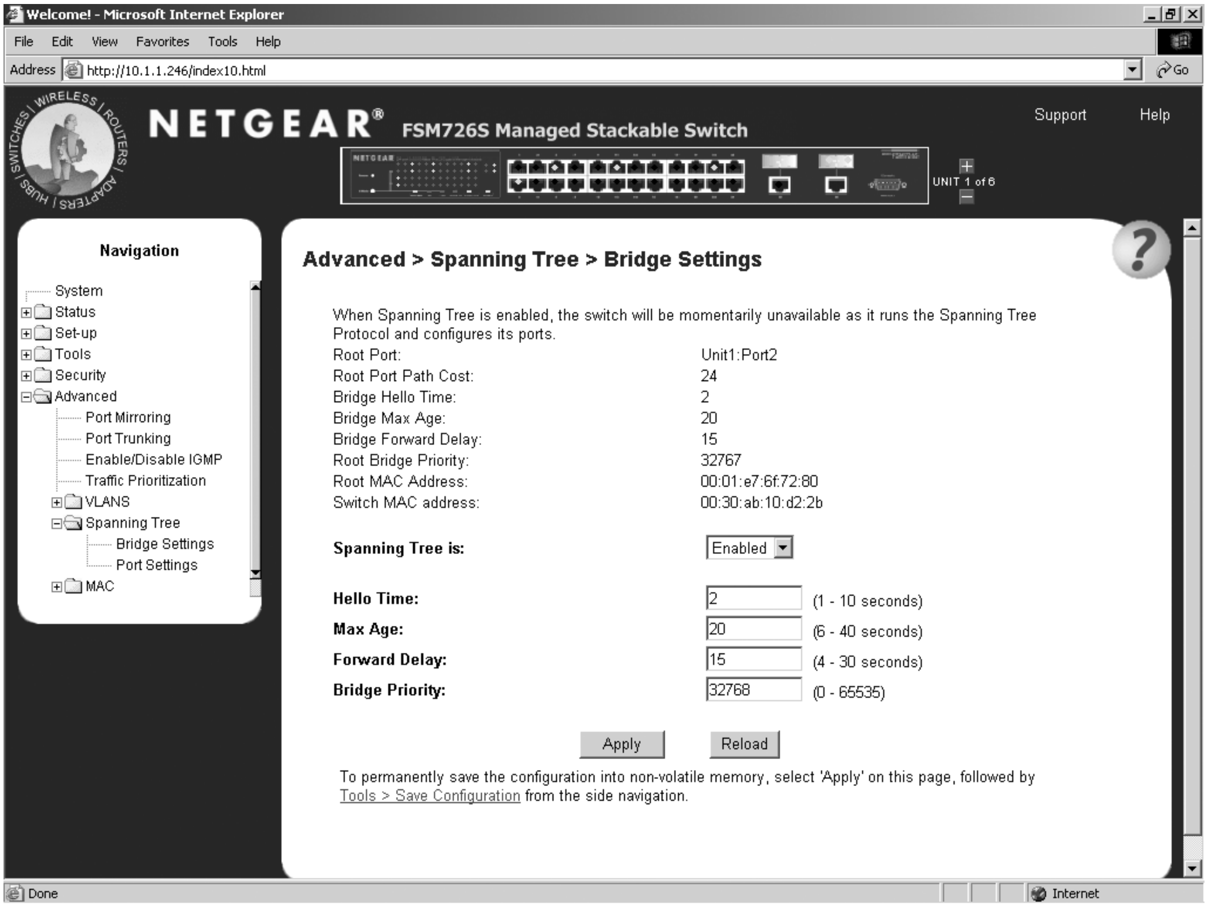
- Root Port
- Root Port Path Cost
- Bridge Hello Time
- Bridge Max Age
- Bridge Forward Delay
- Root Bridge Priority
- Root MAC Address
- Switch MAC Address

Spanning Tree can be enabled or disabled in this screen.

Enable: There are four other tunable parameters to be addressed when enabled.
Hello Time Interval between configuration messages sent by the Spanning Tree algorithm
Max Age Amount of time before a configuration message is discarded by the system
Forward Delay Amount of time system spends in 'learning' and 'listening' states
Bridge Priority Priority setting among other switches in the Spanning Tree

Disable: Disable Spanning Tree algorithm on the system.

When Spanning tree is used in conjunction with a set of aggregated ports, also known as a port trunking, Spanning Tree will treat the trunk as a single virtual port.



Advanced > Spanning Tree > Bridge Settings

When Spanning Tree is enabled, the switch will be momentarily unavailable as it runs the Spanning Tree Protocol and configures its ports.

Root Port:	Unit1:Port2
Root Port Path Cost:	24
Bridge Hello Time:	2
Bridge Max Age:	20
Bridge Forward Delay:	15
Root Bridge Priority:	32767
Root MAC Address:	00:01:e7:6f:72:80
Switch MAC address:	00:30:ab:10:d2:2b

Spanning Tree is: Enabled

Hello Time: 2 (1 - 10 seconds)
Max Age: 20 (6 - 40 seconds)
Forward Delay: 15 (4 - 30 seconds)
Bridge Priority: 32768 (0 - 65535)

Apply Reload

To permanently save the configuration into non-volatile memory, select 'Apply' on this page, followed by Tools > Save Configuration from the side navigation.

Figure 7-23: Spanning Tree: Bridge Settings

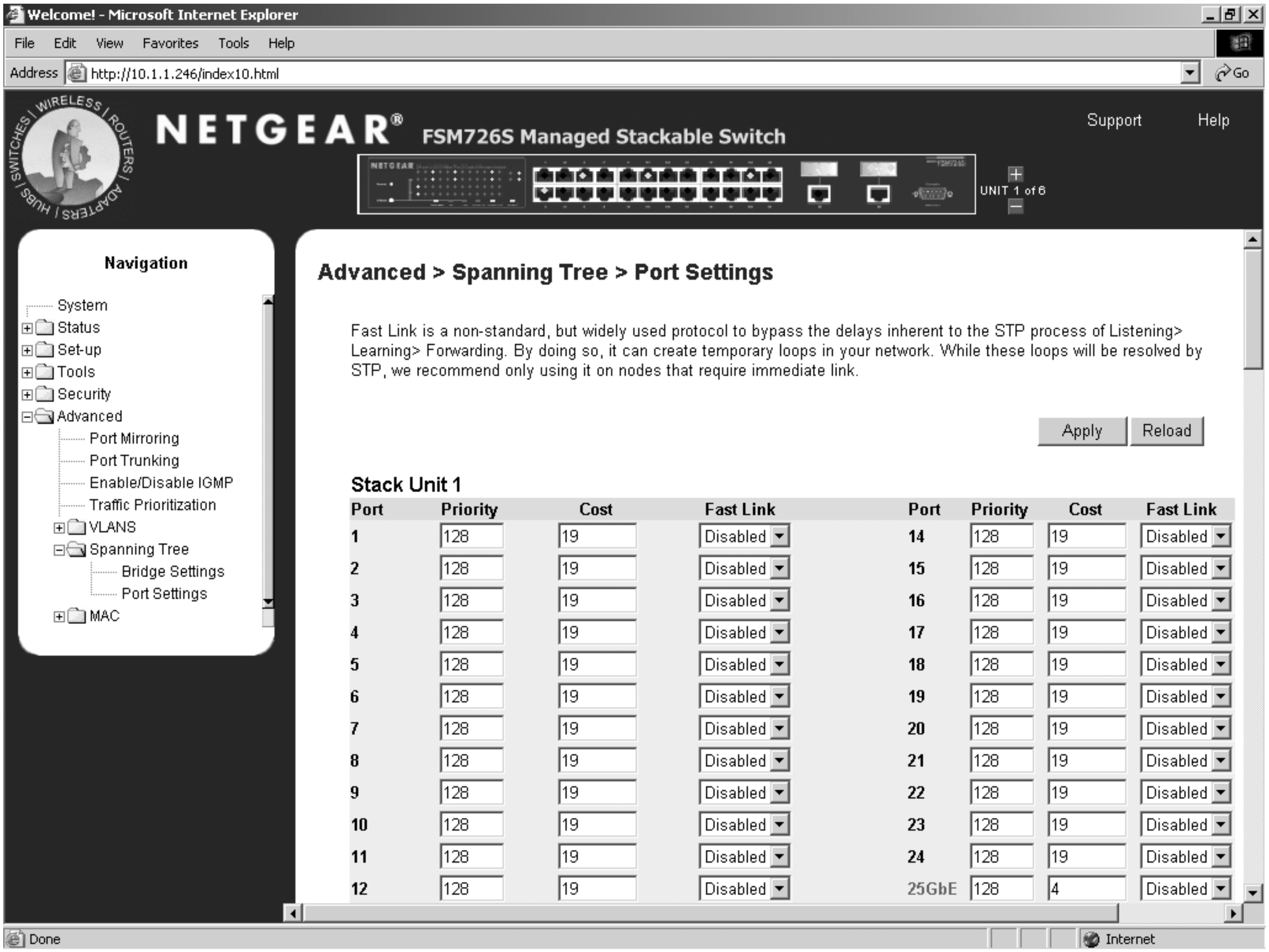
Advanced> Spanning Tree > Port Settings

For the Port Settings options, you can specify Spanning Tree parameters for each port. The Spanning Tree parameters include port priority, path cost, and Fastlink.

Table 7-1. STP Port Setting Parameters

Parameters	Range	Description
Prty (Priority)	0-255	STP bases on this to determine the port to use for forwarding. The port with the lowest number has the highest priority.
Cost	1-65535	The switch uses this to determine which port is the forwarding port. All other factors equal, the path with the lowest cost to the root bridge will be the active path.

Fastlink in STP mode
When a port running the standard STP is connected, it will go through the STP negotiation (listening -> learning -> forwarding or blocking) before it will be fully available. If a server is trying to access a client through the switch running the STP negotiation, it will not be able to connect to it immediately. This can be a problem for some networks. Fastlink mode solves this problem by setting the port directly to forwarding mode, thus allowing any server access request to be forwarded. Fastlink mode can cause temporary loops in your network, but the STP will eliminate them. Fastlink is best used on end node ports, i.e. ports connected to PCs or servers, to avoid network loops.



Advanced > Spanning Tree > Port Settings

Fast Link is a non-standard, but widely used protocol to bypass the delays inherent to the STP process of Listening> Learning> Forwarding. By doing so, it can create temporary loops in your network. While these loops will be resolved by STP, we recommend only using it on nodes that require immediate link.

Stack Unit 1

Port	Priority	Cost	Fast Link	Port	Priority	Cost	Fast Link
1	128	19	Disabled	14	128	19	Disabled
2	128	19	Disabled	15	128	19	Disabled
3	128	19	Disabled	16	128	19	Disabled
4	128	19	Disabled	17	128	19	Disabled
5	128	19	Disabled	18	128	19	Disabled
6	128	19	Disabled	19	128	19	Disabled
7	128	19	Disabled	20	128	19	Disabled
8	128	19	Disabled	21	128	19	Disabled
9	128	19	Disabled	22	128	19	Disabled
10	128	19	Disabled	23	128	19	Disabled
11	128	19	Disabled	24	128	19	Disabled
12	128	19	Disabled	25GbE	128	4	Disabled

Figure 7-24: Spanning Tree: Port Settings

Advanced> MAC

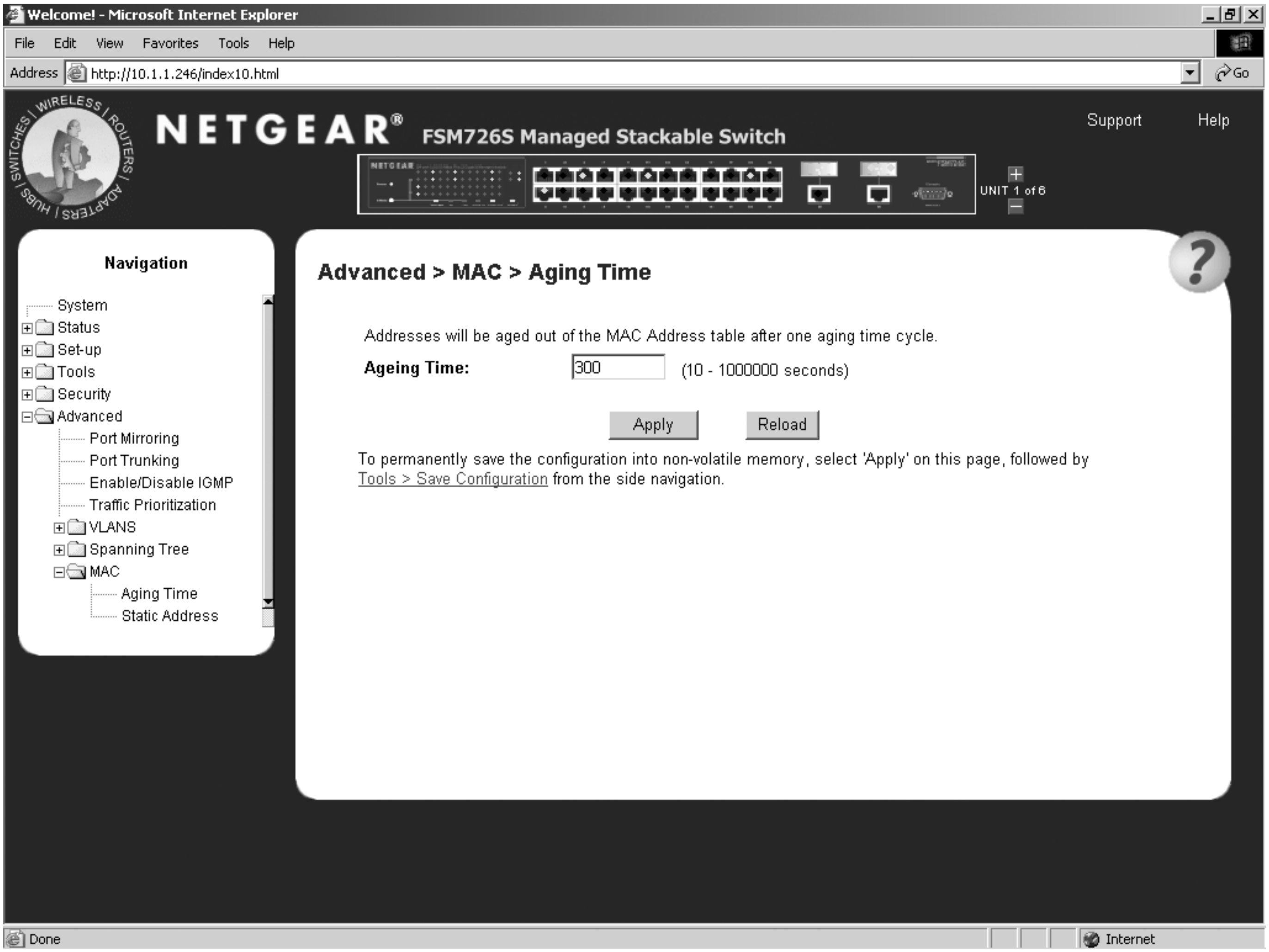
There are two kind of configuration in advanced MAC setup:

- o Aging Time
- o Static Address

Advanced> MAC> Address Aging

Aging Time is a variable that must be configured. Its purpose is to determine the amount of time an entry is held in the forwarding tables while no activity occurs from that address. Entries should be removed to update the table for MAC addresses that have moved or are turned off.
The default value is set to 300 seconds (5 minutes).

- o The administrator may change this value to any value between 10 and 1,000,000 seconds.
- o After changing the value, click 'Apply'



Advanced > MAC > Aging Time

Addresses will be aged out of the MAC Address table after one aging time cycle.

Ageing Time: 300 (10 - 1000000 seconds)

To permanently save the configuration into non-volatile memory, select 'Apply' on this page, followed by Tools > Save Configuration from the side navigation.

Figure 7-25: Address Manager: Address Aging

Advanced> MAC> Static Addresses

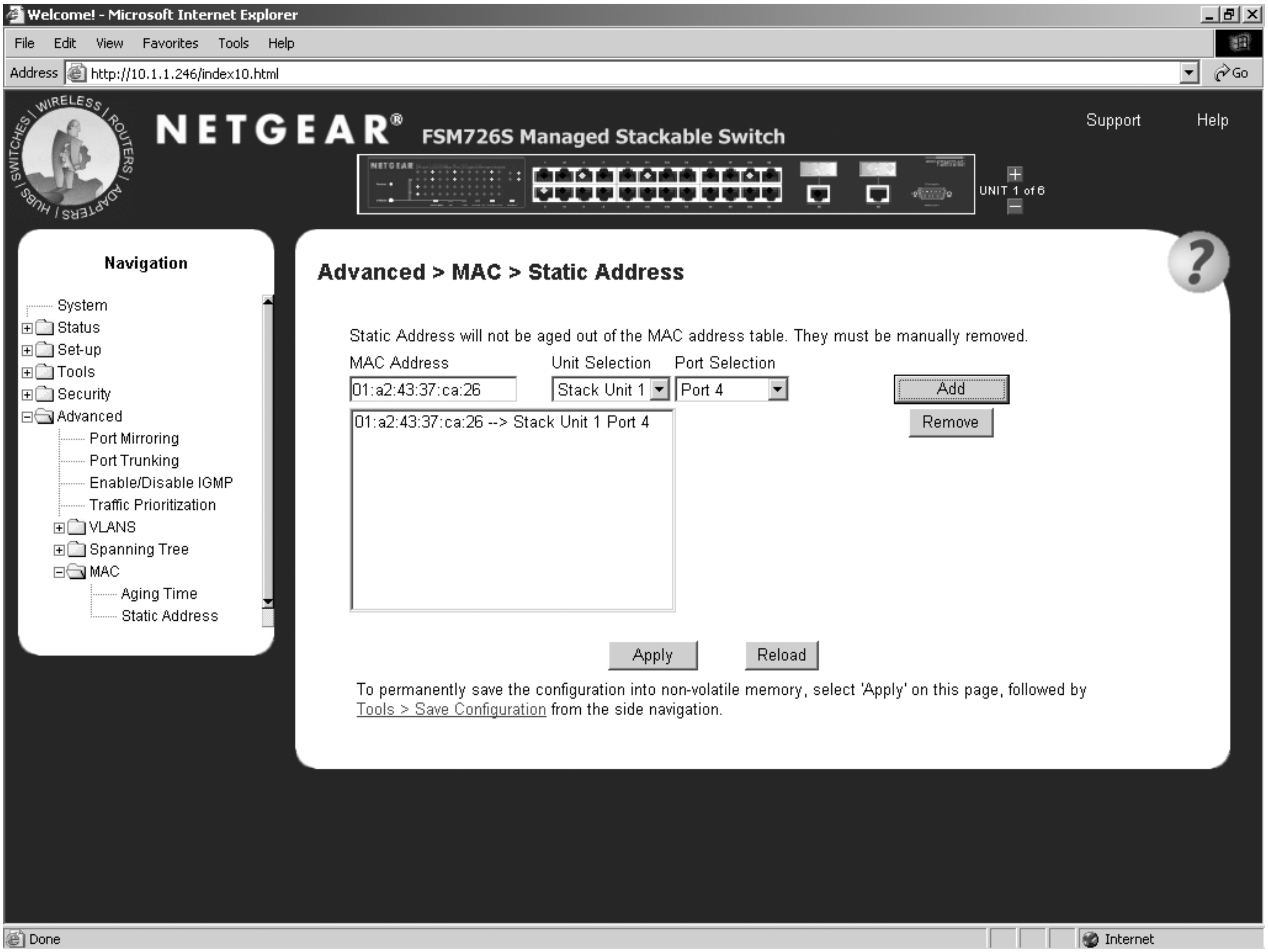
Any system, whose MAC address and the port number are listed in this screen, will not be purged from the system's forwarding table by the aging process.

Add a new entry

- o Enter the MAC address and port in the appropriate boxes
- o Click Add

Remove an exist entry

- o Highlight that entry in the table, by clicking on the MAC address
- o Choose Remove



Advanced > MAC > Static Address

Static Address will not be aged out of the MAC address table. They must be manually removed.

MAC Address: 01:a2:43:37:ca:26
Unit Selection: Stack Unit 1
Port Selection: Port 4

01:a2:43:37:ca:26 --> Stack Unit 1 Port 4

To permanently save the configuration into non-volatile memory, select 'Apply' on this page, followed by Tools > Save Configuration from the side navigation.

Figure 7-26: Address Manager: Static Addresses

Advanced> SNMP

Users can manage this switch by SNMP from a network management station.
SNMP management features on the switch include:

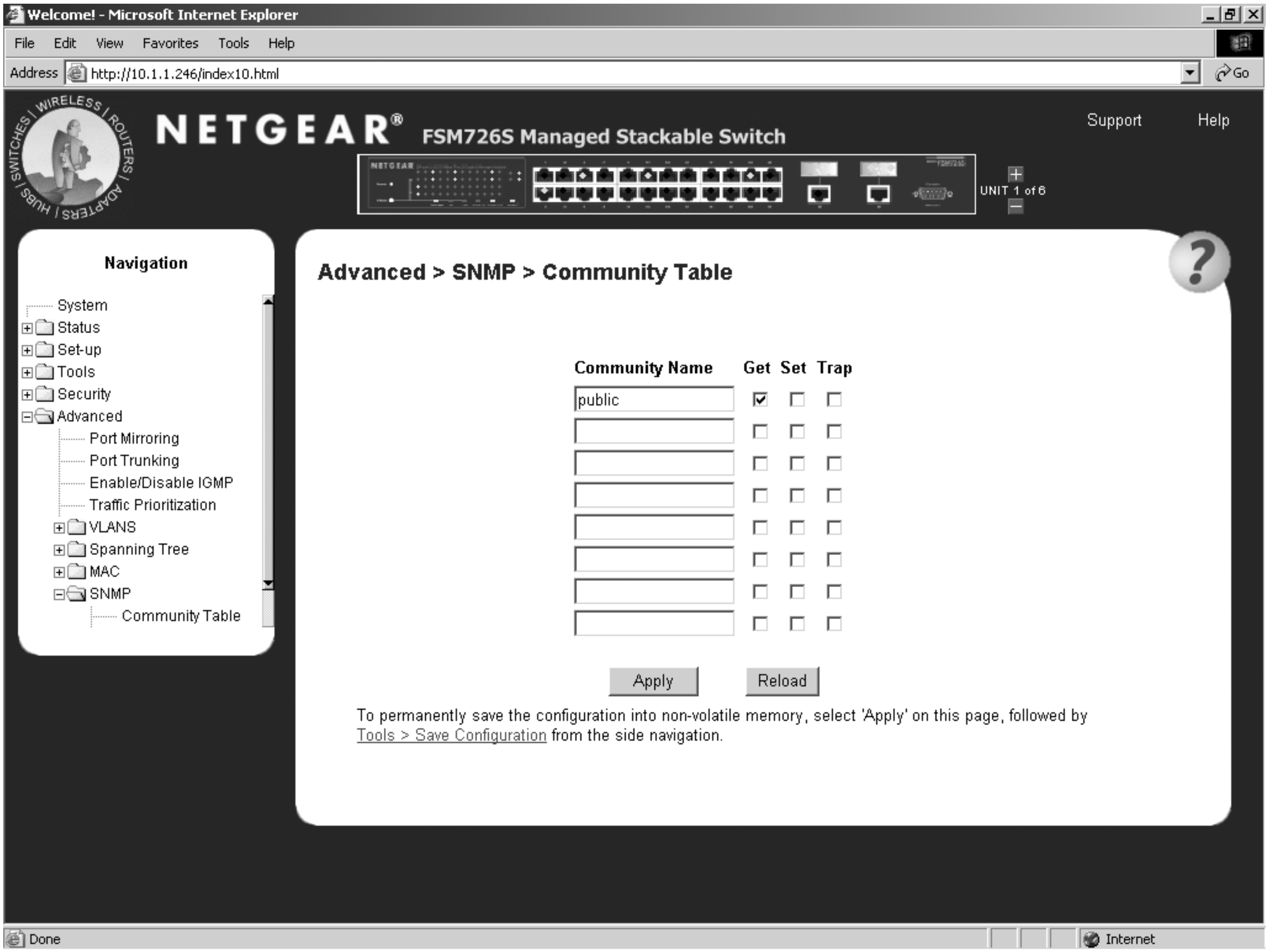
- o Simple Network Management Protocol (SNMP)
- o Support Standard MIBs:
  - MIB II (RFC1213)
  - Ethernet Interface MIB (RFC1643)
  - Bridge MIB (RFC1493)
  - Enterprise MIB
  - 4-Group RMON (RFC1757)

This page has three SNMP Settings:

- o Community Table
- o Host Table
- o Trap Setting

Advanced> SNMP> Community Table

The administrator can create up to eight different community strings with combinations of GET, SET and TRAP privileges. These community strings need to be set prior to setting host access, as the host table depends on the existence of community strings. The public string has GET privileges by default.



Advanced > SNMP > Community Table

Community Name	Get	Set	Trap
public	☑	□	□
	□	□	□
	□	□	□
	□	□	□
	□	□	□
	□	□	□
	□	□	□
	□	□	□

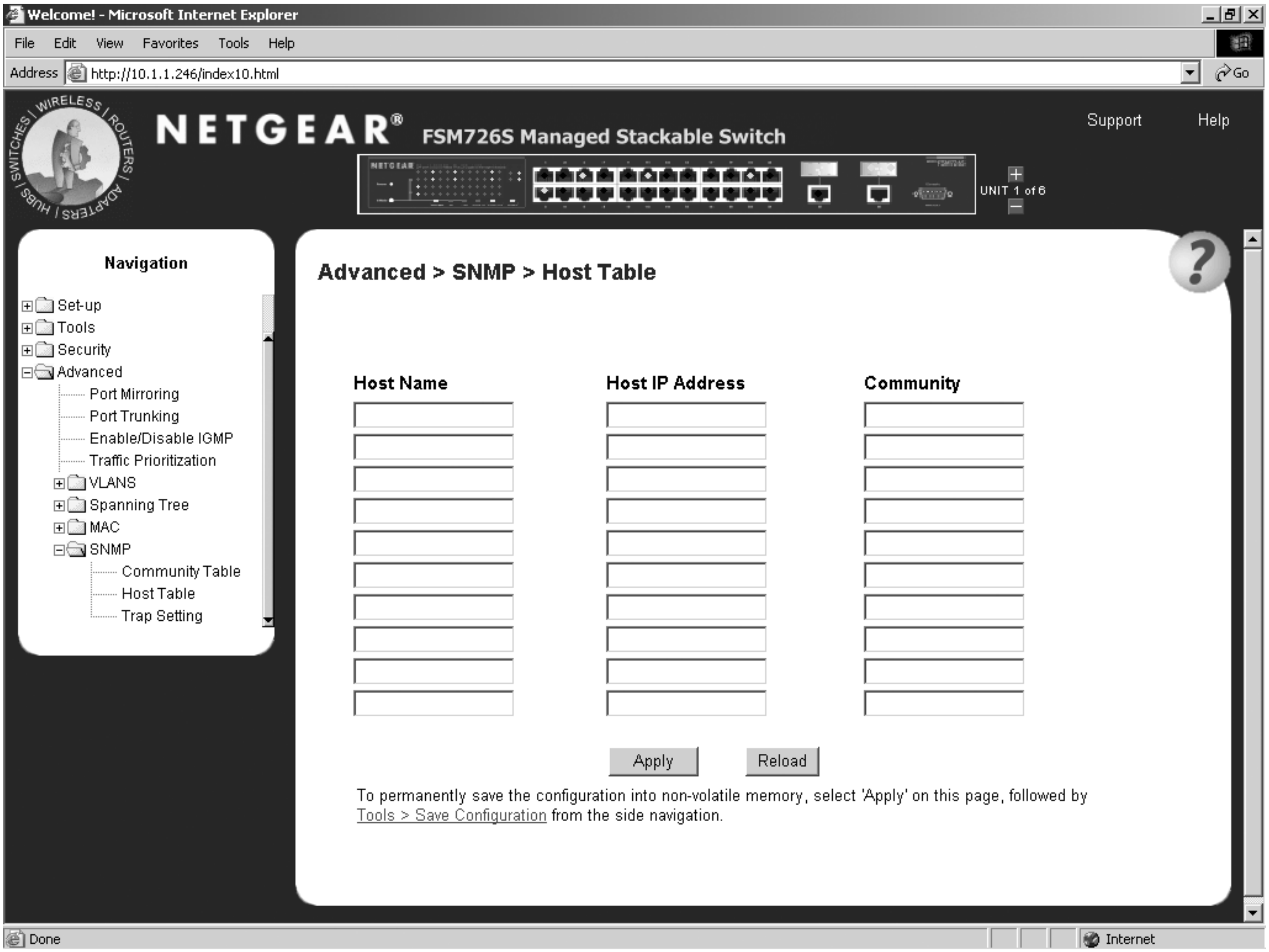
To permanently save the configuration into non-volatile memory, select 'Apply' on this page, followed by Tools > Save Configuration from the side navigation.

Figure 7-27: SNMP Management: Community Table

Advanced> SNMP> Host Table

The SNMP Host Table screen allows you to add and remove hosts from access rights that have been granted to community groups. The permissions GET, SET and TRAP are assigned to a community name and then these permissions are assigned to individual machines by adding those machines and their IP address to the appropriate community string. Host Authorization can be Enabled or Disabled.

If Host Authorization is enabled, the host must be added to this table, through the Console port connection in order for an end station to be access the switch via SNMP.



Advanced > SNMP > Host Table

Host Name	Host IP Address	Community

To permanently save the configuration into non-volatile memory, select 'Apply' on this page, followed by Tools > Save Configuration from the side navigation.

Figure 7-28: SNMP Management: Host Table

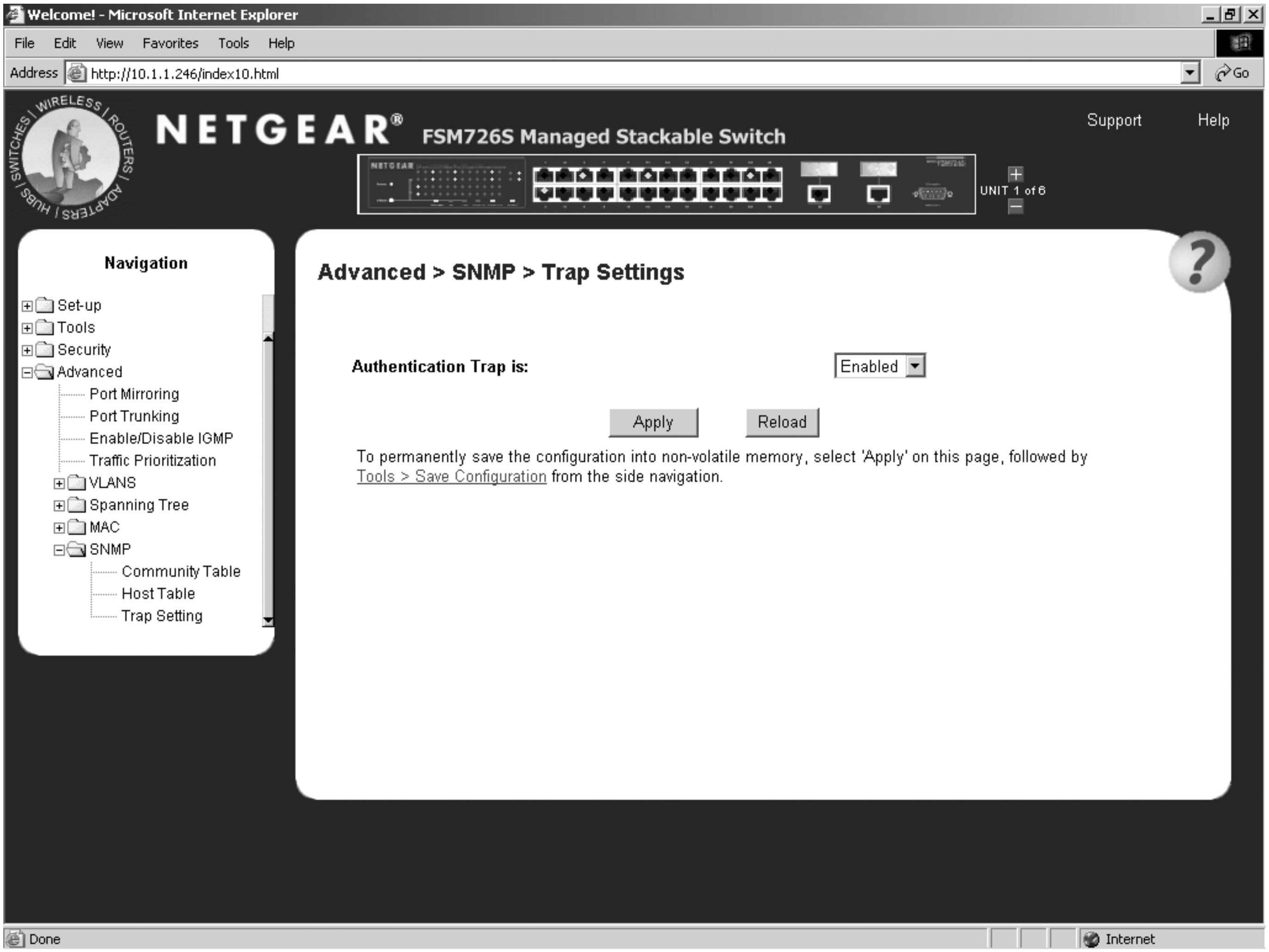
Advanced> SNMP> Trap Setting

When on, the system will generate an SNMP trap upon a host authorization failure. This failure occurs when a host tries to gain access to the system but the host's IP is not in the SNMP host table.

Authentication traps

- o Enable The system will generate a SNMP trap upon a host authorization failure
- o Disable The authentication traps will not be generated

All hosts in community strings with TRAP privileges will be notified when a trap condition occurs.



Advanced > SNMP > Trap Settings

Authentication Trap is: Enabled

To permanently save the configuration into non-volatile memory, select 'Apply' on this page, followed by Tools > Save Configuration from the side navigation.

Figure 7-29: SNMP Management: Trap Settings

APPENDIX A: GLOSSARY

This appendix defines terms associated with switching technology.

10BASE-T	The IEEE specification for 10 Mbps Ethernet over Category 3, 4, or 5 twisted-pair cable.
100BASE-FX	The IEEE specification for 100 Mbps Fast Ethernet over fiber-optic cable.
100BASE-TX	The IEEE specification for 100 Mbps Fast Ethernet over Category 5 twisted-pair cable.
1000BASE-SX	The IEEE specification for 1000 Mbps Gigabit Ethernet over fiber-optic cable.
1000BASE-T	The IEEE specification for 1000 Mbps Gigabit Ethernet over Category 5 twisted-pair cable.
Auto-negotiation	A feature that allows twisted-pair ports to advertise their capabilities for speed, duplex and flow control. When connected to a port that also supports auto-negotiation, the link can automatically configure itself to the optimum setup.
Auto Uplink	A feature that allows twisted-pair ports to sense if a normal (MDI-X) or uplink (MDI) connection is necessary and make the right link. It adjusts for straight-through or crossover cables.
Backbone	The part of a network used as a primary path for transporting traffic between network segments.
Bandwidth	The information capacity, measured in bits per second, that a channel could transmit. Bandwidth examples include 10 Mbps for Ethernet, 100 Mbps for Fast Ethernet, and 1000 Mbps (I Gbps) for Gigabit Ethernet.
Baud	The signaling rate of a line, that is, the number of transitions (voltage or frequency changes) made per second. Also known as line speed.
Broadcast	A packet sent to all devices on a network.
Broadcast storm	Multiple simultaneous broadcasts that typically absorb all the available network bandwidth and can cause a network to fail. Broadcast storms can be due to faulty network devices or network loops.
Capacity planning	Determining whether current solutions can satisfy future demands. Capacity planning includes evaluating potential workload and infrastructure changes.
Class of Service	A term to describe treating different types of traffic with different levels of service priority. Higher priority traffic gets faster treatment during times of switch congestion
Collision	A term used to describe two colliding packets in an Ethernet network. Collisions are a part of normal Ethernet operation, but a sudden prolonged increase in the number of collisions can indicate a problem with a device, particularly if it is not accompanied by a general increase in traffic.
Endstation	A computer, printer, or server that is connected to a network.
Ethernet	A LAN specification developed jointly by Xerox, Intel and Digital Equipment Corporation. Ethernet networks transmit packets at a rate of 10 Mbps.
Fast Ethernet	An Ethernet system that is designed to operate at 100 Mbps.
Gigabit Ethernet	An Ethernet system that is designed to operate at 1000 Mbps (1 Gbps).
Fault isolation	A technique for identifying and alerting administrators about connections (such as those associated with switch ports) that are experiencing congestion or failure, or exceeding an administrator-defined threshold.
Forwarding	The process of sending a packet toward its destination using a networking device.
Filtering	The process of screening a packet for certain characteristics, such as source address, destination address, or protocol. Filtering is used to determine whether traffic is to be forwarded, and can also prevent unauthorized access to a network or network devices.
Flow control	A congestion- control mechanism. Congestion is caused by devices sending traffic to already overloaded port on a switch. Flow control prevents packet loss and temporarily inhibits devices from generating more traffic until the period of congestion ends.
Full-duplex	A system that allows packets to be transmitted and received at the same time and, in effect, doubles the potential throughput of a link.
Half-duplex	A system that allows packets to transmitted and received, but not at the same time. Contrast with full-duplex.
IEEE	Institute of Electrical and Electronics Engineers. This American

	organization was founded in 1963 and sets standards for computers and communications.
IETF	Internet Engineering Task Force. An organization responsible for providing engineering solutions for TCP/IP networks. In the network management area, this group is responsible for the development of the SNMP protocol.
IGMP	Internet Group Management Protocol, the standard for IP multicasting in the Internet. IGMP is used to establish host memberships in multicast groups on a single network. (See IP multicast)
IP	Internet Protocol. IP is a layer 3 network protocol that is the standard for sending data through a network. IP is part of the TCP/IP set of protocols that describe the routing of packets to addressed devices.
IP address	Internet Protocol address. A unique identifier for a device attached to a network using TCP/IP. The address is written as four octets separated with periods (full-stops), and is made up of a network section, an optional subnet section and a host section.
IP multicast	Sending data to distributed servers on a multicast backbone. For large amounts of data, IP Multicast is more efficient than normal Internet transmissions, because the server can broadcast a message to many recipients simultaneously. Unlike traditional Internet traffic that requires separate connections for each source-destination pair, IP multicasting allows many recipients to share the same source. This means that just one set of packets is transmitted for all the destinations.
LAN	Local Area Network. A network of endstations (such as PCs, printers, servers) and network devices (hubs and switches) that cover a relatively small geographic area (usually not larger than a floor or building).
Load balancing	The ability to distribute traffic across various ports of a device, such as a switch, to provide efficient, optimized traffic throughout the network.
Loop	An event that occurs when two network devices are connected by more than one path, thereby causing packets to repeatedly cycle around the network and not reach their destination.
MAC	Media Access Control. A protocol specified by the IEEE for determining which devices have access to a network at any one time.
MAC address	Media Access Control address; also called hardware or physical address. Most devices that connect to a LAN have a MAC address assigned to them, as they are used to identify other devices in a network.
Multicast	A single packet sent to a specific group of endstations on a network.
Port monitoring	The ability to monitor the traffic passing through a port on a device to analyze network characteristics and perform troubleshooting.
Port speed	The speed that a port on a device uses to communicate with another device or the network.
Port trunking	The ability to combine multiple ports on a device to create a single, high-bandwidth connection.
Protocol	A set of rules for communication between devices on a network.
Quality of Service	A term to describe delay, throughput, bandwidth, and other factors that measure the service quality provided to a user.
Segment	A section of a LAN that is connected to the rest of the network using a switch, bridge, or repeater.
SNMP	Simple Network Management Protocol. An IETF standard protocol for managing devices on a TCP/IP network.
Spanning Tree	A technique that detects loops in a network and logically blocks the redundant paths, ensuring that only one route exists between any two LANs.
Spanning Tree Protocol (STP)	A protocol that finds the most efficient path between segments of a multi-looped, bridged network. STP allows redundant switches and bridges to be used for network resilience, without the broadcast storms associated with looping. If a switch or bridge falls, a new path to a redundant switch or bridge is opened.
Switch	A device that interconnects several LANs to form a single logical LAN that comprises of several LAN segments. Switches are similar to bridges, in that they connect LANs of a different type; however they connect more LANs than a bridge and are generally more sophisticated.
TCP/IP	Transmission Control Protocol/Internet Protocol. This is the name for two of the most well-known protocols developed for the interconnection of networks. Originally a UNIX standard, TCP/IP is now supported on almost all platforms, and is the protocol of the Internet. ■ TCP relates to the content of the data traveling through a network

	— ensuring that the information sent arrives in one piece when it reaches its destination. ■ IP relates to the address of the endstation to which data is being sent, as well as the address of the destination network.
Telnet	A TCP/IP application protocol that provides a virtual terminal service, allowing a user to log into another computer system and access a device as if the user were connected directly to the device.
TFTP	Trivial File Transfer Protocol. Allows you to transfer files (such as software upgrades) from a remote device using the local management capabilities of the Switch.
Traffic prioritization	Giving time-critical data traffic a higher quality of service over other, non-critical data traffic.
Unicast	A packet sent to a single endstation on a network.
VLAN	Virtual LAN. A logical association that allows users to communicate as if they were physically connected to a single LAN, independent of the actual physical configuration of the network.

APPENDIX B: TROUBLESHOOTING

This chapter provides information about troubleshooting the NETGEAR Model FSM726S Managed Stackable Switch. Topics include:

- Troubleshooting chart
- Additional troubleshooting suggestions

Troubleshooting Chart

Table B-1 lists symptoms, causes, and solutions of possible problems.

Table B-1. Troubleshooting Chart

Symptom	Cause	Solution
Power LED is off.	No power is received	Check the power cord connections for the switch at the switch and the connected device. Make sure all cables used are correct and comply with Ethernet specifications.
Link LED is off or intermittent.	Port connection is not working.	Check the crimp on the connectors and make sure that the plug is properly inserted and locked into the port at both the switch and the connecting device. Make sure all cables used are correct and comply with Ethernet specifications. See Appendix D. Check for a defective adapter card, cable, or port by testing them in an alternate environment where all products are functioning.
File transfer is slow or performance degradation is a problem.	Half- or full-duplex setting on the switch and the connected device are not the same.	Make sure the attached device is set to auto negotiate.
A segment or device is not recognized as part of the network.	One or more devices are not properly connected, or cabling does not meet Ethernet guidelines.	Verify that the cabling is correct. Be sure all connectors are securely positioned in the required ports. Equipment may have been accidentally disconnected.
FDX LED is blinking yellow excessively.	Collisions are occurring on the connected segment. Duplex modes are mismatched.	Some collisions are normal when the connection is operating in half-duplex mode. Recheck the settings of the device attached to the RJ-45 port. Make sure the attached device is set to auto negotiate.
ACT LED is flashing continuously on all connected ports and the network is disabled	A network loop (redundant path) has been created (see Figure 2-3).	Break the loop by ensuring that there is only one path from any networked device to any other networked device.

Additional Troubleshooting Suggestions

If the suggestions in Table B-1 do not resolve your problem, refer to the troubleshooting suggestions in this section.

Network Adapter Cards

Make sure the network adapter cards installed in the PCs are in working condition and the software driver has been installed.

Configuration

If problems occur after altering the network configuration, restore the original connections and determine the problem by implementing the new changes, one step at a time. Make sure that cable distances, repeater limits, and other physical aspects of the installation do not exceed the Ethernet limitations.

Switch Integrity

If required, verify the integrity of the switch by resetting the switch. To reset the switch, use the Tools> Reset command or remove AC power from the switch and then reapply AC power. If the problem continues, contact NETGEAR technical support. In North America, call 1-888-NETGEAR. If you are outside of North America, please refer to the support information card included with your product.

Auto Negotiation

The 10/100 Mbps ports negotiate the correct duplex mode and speed if the device at the other end of the link supports auto negotiation. If the device does not support auto negotiation, the switch only determines the speed correctly and the duplex mode defaults to half-duplex.

The gigabit port on the Gigabit module negotiates speed, duplex mode, and flow control, provided that the attached device supports auto-negotiation.

APPENDIX C: Virtual Local Area Network (VLAN)

A Local Area Network (LAN) can generally be defined as a broadcast domain. Hubs, bridges or switches in the same physical segment or segments connect all end node devices. End nodes can communicate with each other without the need for a router. Routers connect LANs together, routing the traffic to appropriate port.

A virtual LAN (VLAN) is a local-area network with a definition that maps workstations on some other basis than geographic location (for example, by department, type of user, or primary application). To communicate between VLANs, traffic must go through a router, just as if they were on two separate LANs.

A VLAN is a group of PCs, servers and other network resources that behave as if they were connected to a single, network segment — even though they may not be. For example, all marketing personnel may be spread throughout a building. Yet if they are all assigned to a single VLAN, they can share resources and bandwidth as if they were connected to the same segment. The resources of other departments can be invisible to the marketing VLAN members, accessible to all, or accessible only to specified individuals, depending on how the IT manager has set up the VLANs.

The Advantages of VLANs

Easy to do network segmentation

Users communicate most frequently with each other can be grouped into common VLANs, regardless of physical location. Each group's traffic is largely contained within the VLAN, reducing extraneous traffic and improving the efficiency of the whole network.

Easy to manage

The addition of nodes, as well as moves and other changes, can be dealt with quickly and conveniently from a management interface rather than the wiring closet.

Increased performance

VLANs free up bandwidth by limiting node-to-node and broadcast traffic throughout the network.

Enhanced network security

VLANs create virtual boundaries that can only be crossed through a router. So standard, router-based security measures can be used to restrict access to each VLAN

VLAN Behavior in the FSM726S

Packets received by the switch will be treated in the following way:

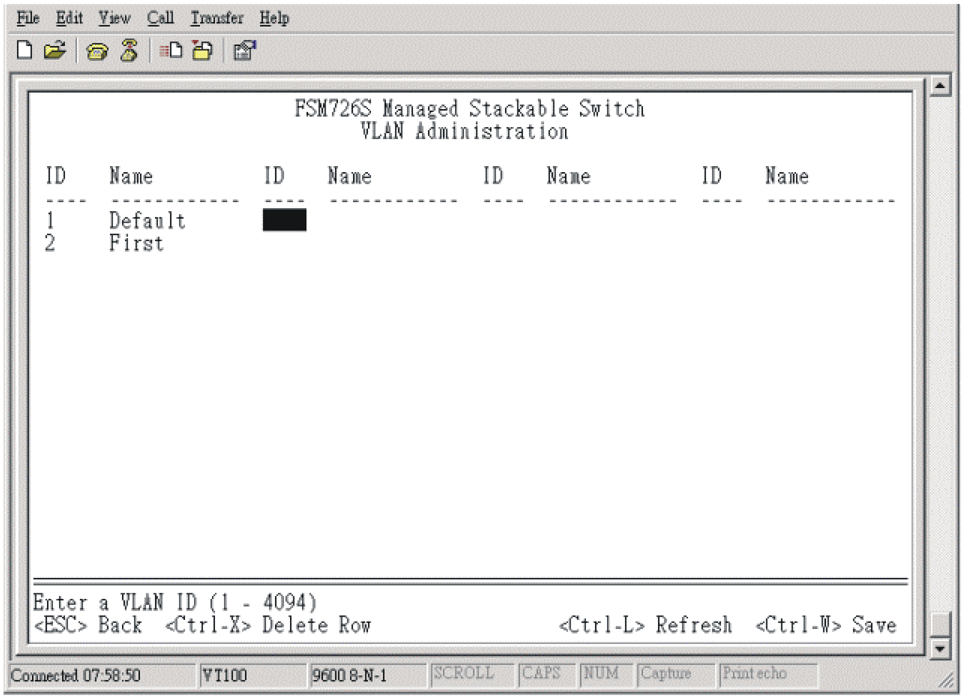
- When an untagged packet enters a port, it will be automatically tagged with the port's default VLAN ID tag number. Each port has a default VLAN ID setting that is user configurable (the default setting is 1). The default VLAN ID setting for each port can be changed in that port's respective Port Configuration page.
- When a tagged packet enters a port, the tag for that packet will be unaffected by the default VLAN ID Setting.
- The packet will now proceed to the VLAN specified by its VLAN ID tag number.
- If the port in which the packet entered does not have membership with the VLAN specified by the VLAN ID tag, the packet will be dropped. Port VLAN membership settings are changed in the Primary VLAN page.
- If the port has membership to the VLAN specified by the packet's VLAN ID, the packet will be able to be sent to other ports with the same VLAN ID membership.
- Packets leaving the switch will be either tagged or untagged depending on the setting for that port's VLAN membership properties.
    - A 'U' for a given port and VLAN will mean that packets leaving the switch from that port and VLAN will be Untagged. Inversely, a 'T' for a given port and VLAN will mean that packets leaving the switch from that port and VLAN will be tagged with the respective VLAN ID in which it participated in.

Two examples of for setting up VLANs will be given. Example 1 will step through a simple two-group VLAN setup. Example 2 will step through a more elaborate setup illustrating all possible scenarios for a comprehensive understanding of tagged VLANs.

Example 1

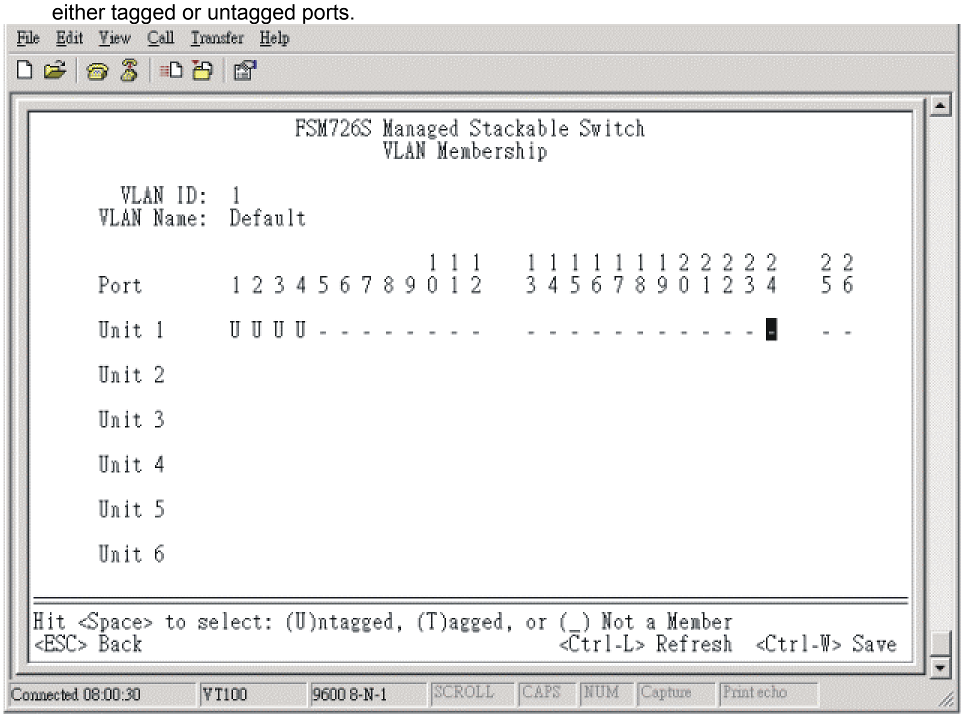
This example shows the basics of setting up a VLAN.

1. In the VLAN Administration page, add a new VLAN to the list, shown below as “First” with a VLAN ID value of 2.

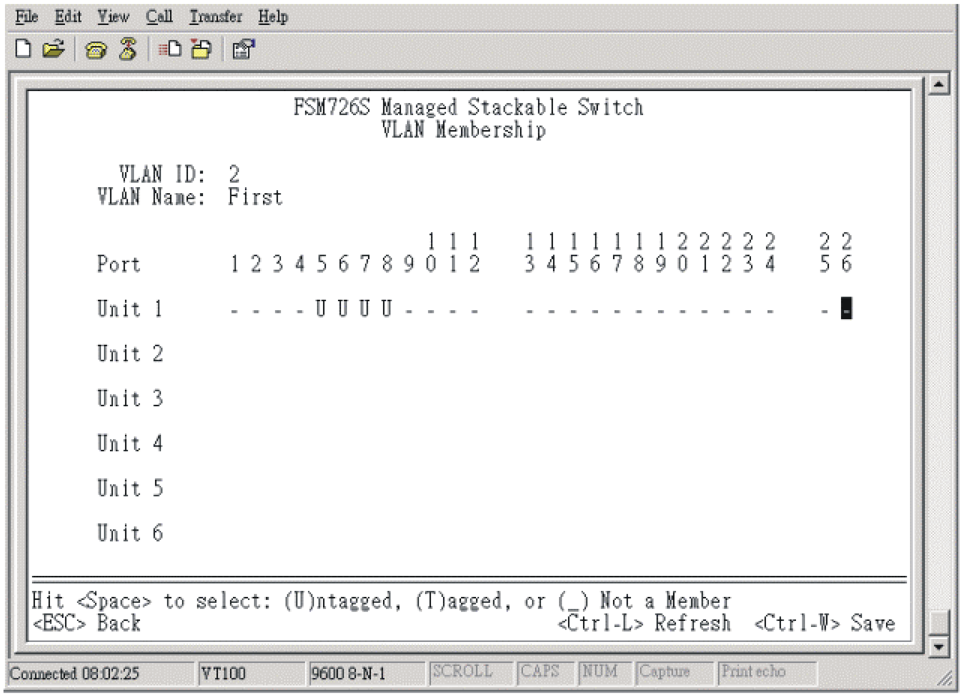


```
                        FSM726S Managed Stackable Switch
                              VLAN Administration

 ID    Name          ID    Name          ID    Name          ID    Name
 ----  ------------  ----  ------------  ----  ------------  ----  ------------
 1     Default       █
 2     First










Enter a VLAN ID (1 - 4094)
<ESC> Back  <Ctrl-X> Delete Row                        <Ctrl-L> Refresh  <Ctrl-W> Save
```

2. In the VLAN Membership page, use the space bar to modify the matrix until the desired ports are all members of the selected VLAN as either tagged or untagged ports.

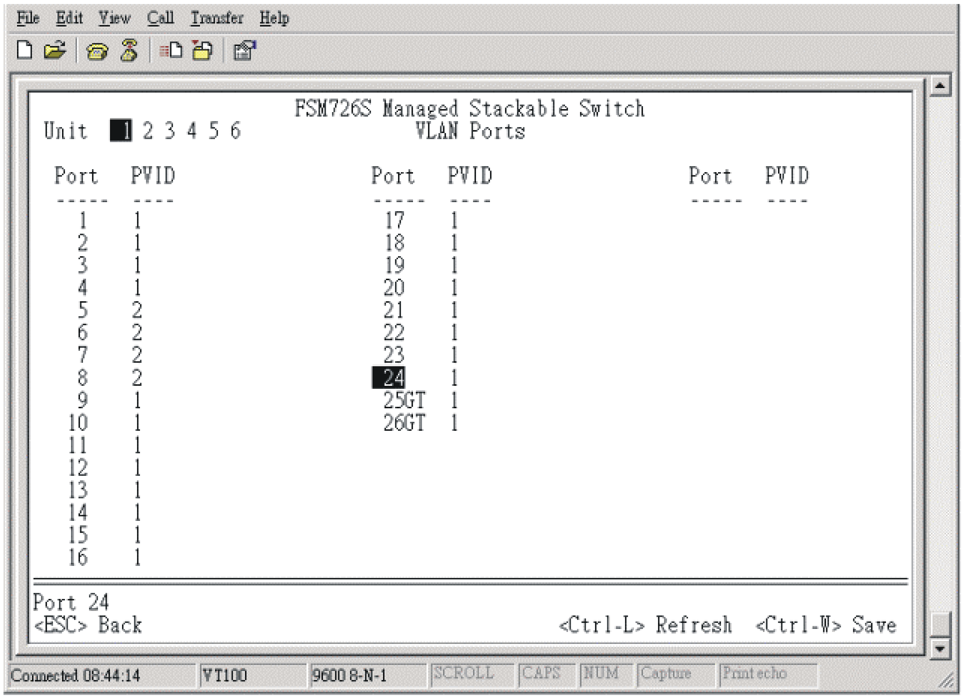


```
                        FSM726S Managed Stackable Switch
                                VLAN Membership

      VLAN ID:  1
    VLAN Name:  Default

                                    1 1 1     1 1 1 1 1 1 2 2 2 2 2     2 2
    Port        1 2 3 4 5 6 7 8 9 0 1 2     3 4 5 6 7 8 9 0 1 2 3 4     5 6

    Unit 1      U U U U - - - - - - - -     - - - - - - - - - - - -     - -

    Unit 2

    Unit 3

    Unit 4

    Unit 5

    Unit 6

Hit <Space> to select: (U)ntagged, (T)agged, or (_) Not a Member
<ESC> Back                                             <Ctrl-L> Refresh  <Ctrl-W> Save
```



```
                     FSM726S Managed Stackable Switch
                             VLAN Membership

     VLAN ID:  2
    VLAN Name:  First

                                   1 1 1   1 1 1 1 1 1 2 2 2 2 2   2 2
    Port        1 2 3 4 5 6 7 8 9 0 1 2   3 4 5 6 7 8 9 0 1 2 3 4   5 6

    Unit 1      - - - - U U U U - - - -   - - - - - - - - - - - -   - -

    Unit 2

    Unit 3

    Unit 4

    Unit 5

    Unit 6

Hit <Space> to select: (U)ntagged, (T)agged, or (_) Not a Member
<ESC> Back                                <Ctrl-L> Refresh  <Ctrl-W> Save
```

3. To allow untagged packets to participate in the 'First' VLAN, make sure to change the Port VLAN IDs for the relevant ports. Access the PVID Settings page then use the space bar to add an 'X' indicating which Port VLAN ID is assigned to which port.

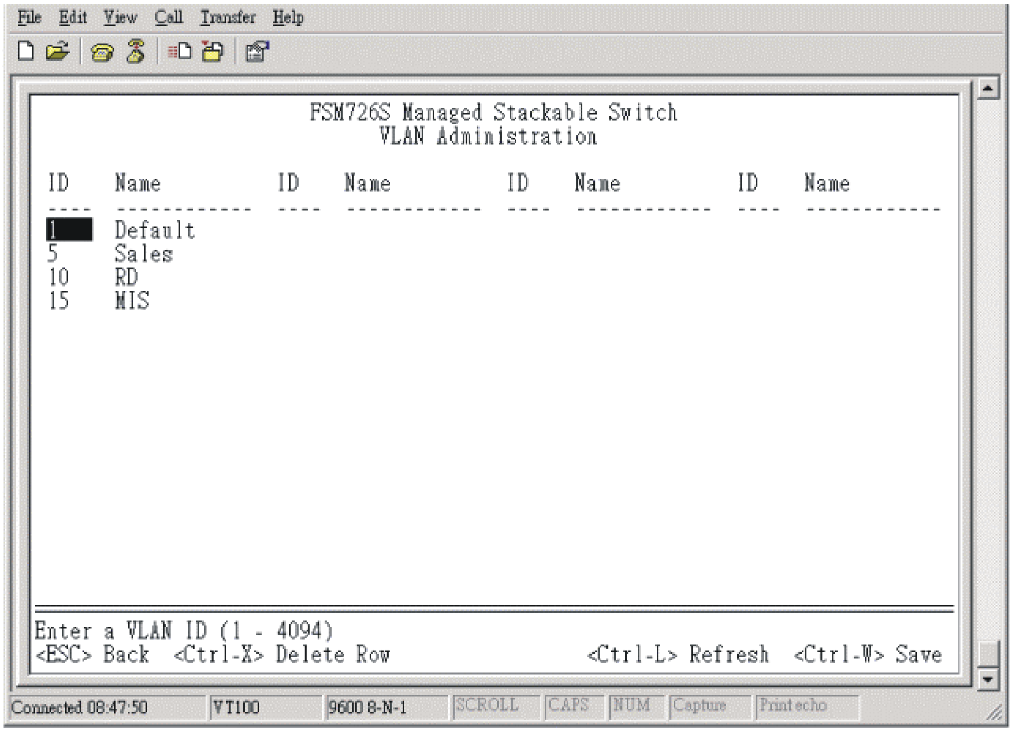


```
                     FSM726S Managed Stackable Switch
 Unit  1 2 3 4 5 6                VLAN Ports

  Port   PVID                 Port   PVID                 Port   PVID
  -----  ----                 -----  ----                 -----  ----
    1     1                    17     1
    2     1                    18     1
    3     1                    19     1
    4     1                    20     1
    5     2                    21     1
    6     2                    22     1
    7     2                    23     1
    8     2                    24     1
    9     1                    25GT   1
   10     1                    26GT   1
   11     1
   12     1
   13     1
   14     1
   15     1
   16     1

Port 24
<ESC> Back                                <Ctrl-L> Refresh  <Ctrl-W> Save
```

Example 2

This example demonstrates several scenarios of VLAN use and how the switch will handle VLAN and non-VLAN traffic.

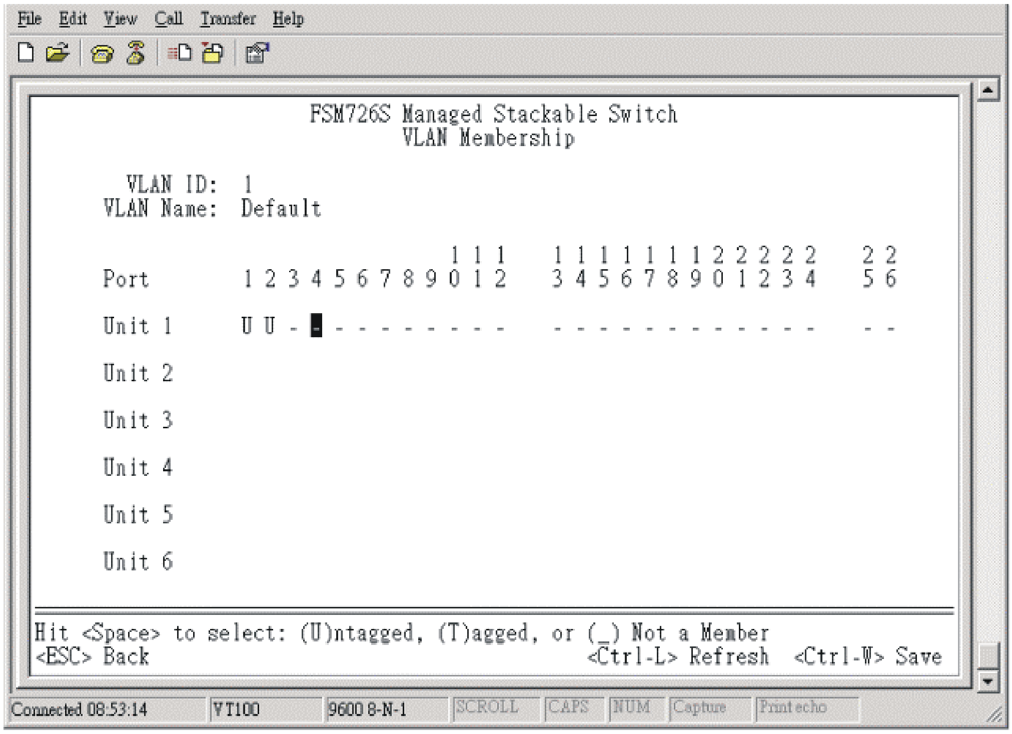
1) Setup the following VLANs:



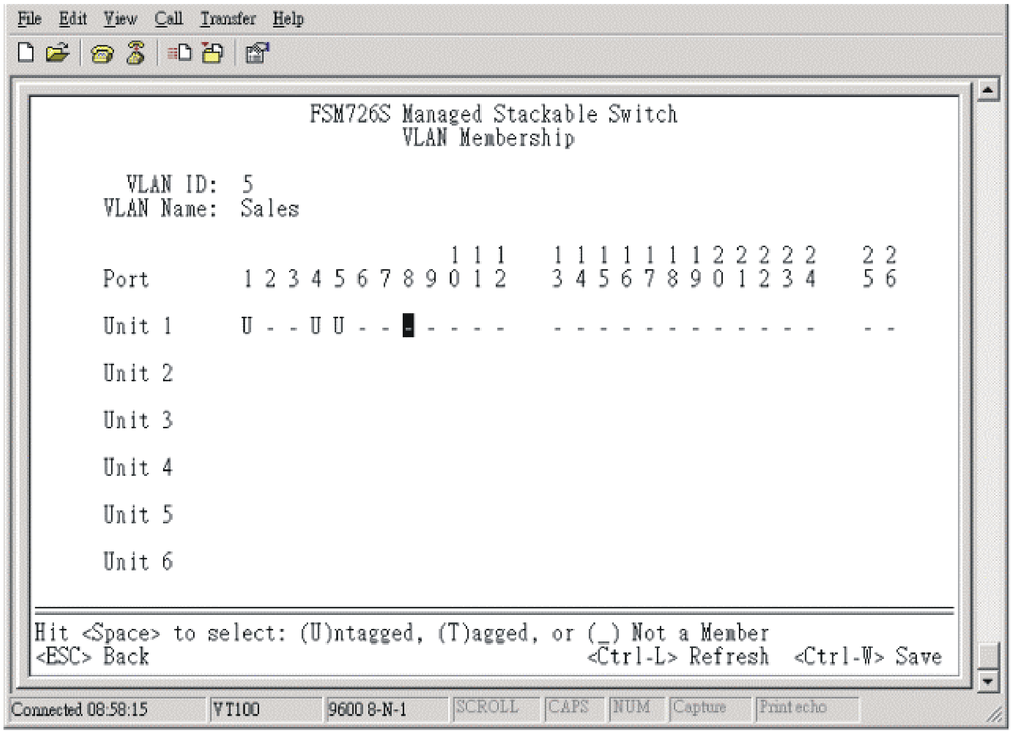
```
                    FSM726S Managed Stackable Switch
                          VLAN Administration

ID    Name          ID    Name          ID    Name          ID    Name
----  ------------  ----  ------------  ----  ------------  ----  ------------
1     Default
5     Sales
10    RD
15    MIS

Enter a VLAN ID (1 - 4094)
<ESC> Back  <Ctrl-X> Delete Row                <Ctrl-L> Refresh  <Ctrl-W> Save
```

2) Configure the VLAN membership. Each image below shows a different VLAN to be setup. Be sure to set all of them as follows.

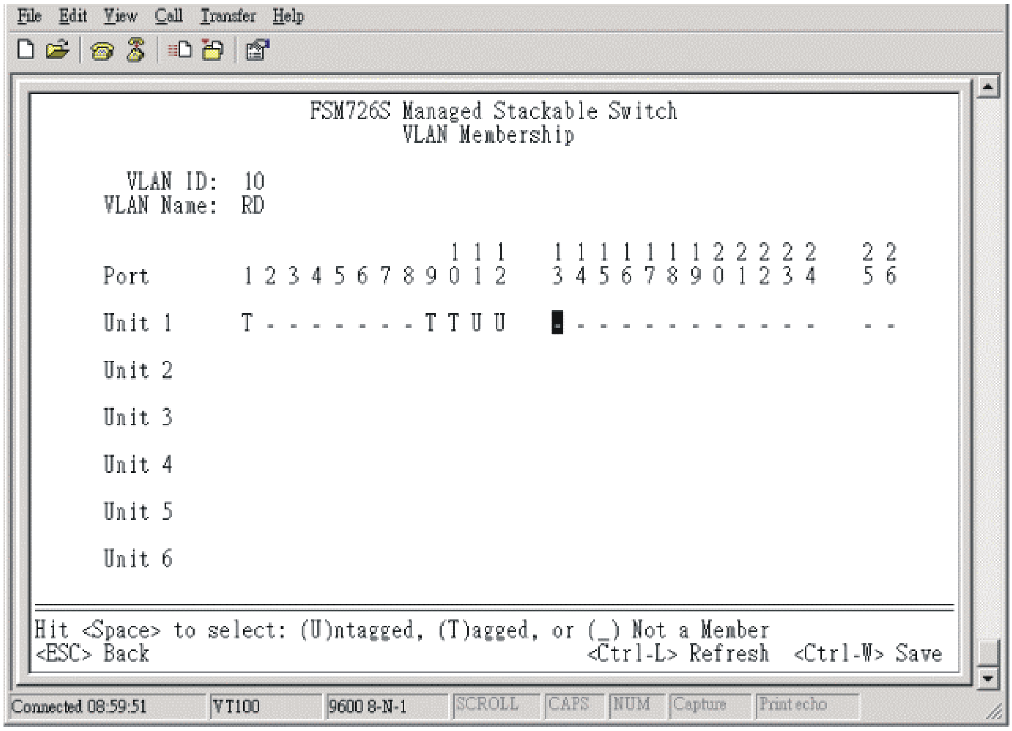
Note: this example uses a single switch, but the same principles apply to a VLAN that had ports on several switches in a stack



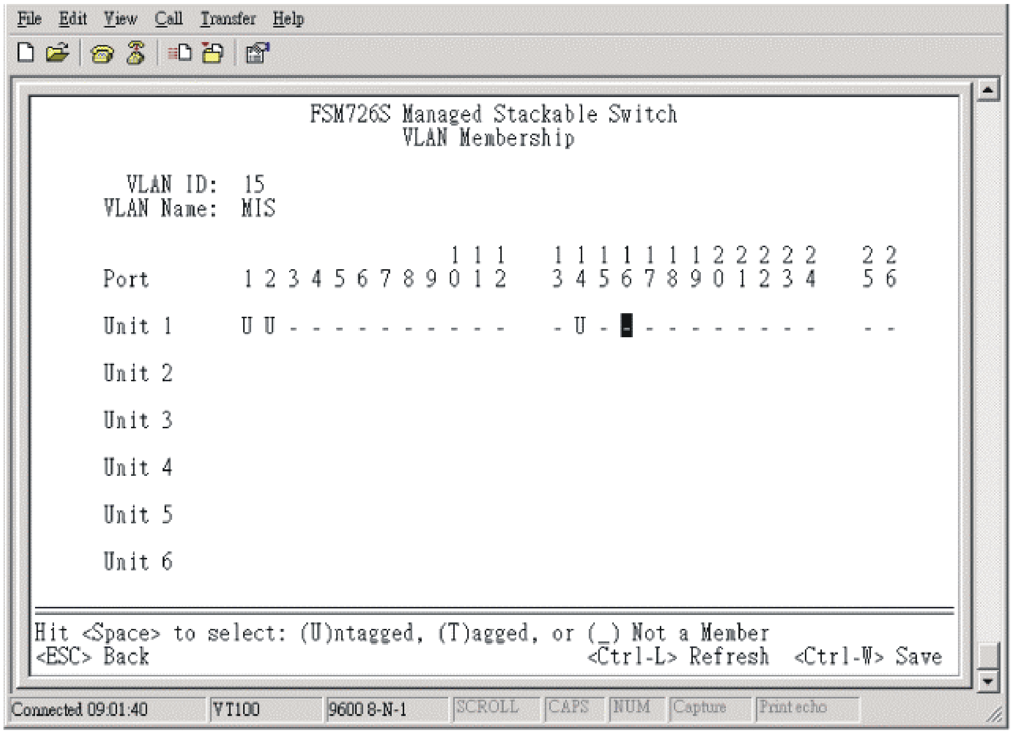
```
                        FSM726S Managed Stackable Switch
                                VLAN Membership

        VLAN ID:  1
      VLAN Name:  Default

                                    1 1 1    1 1 1 1 1 1 1 2 2 2 2 2   2 2
      Port        1 2 3 4 5 6 7 8 9 0 1 2    3 4 5 6 7 8 9 0 1 2 3 4   5 6

      Unit 1      U U - - - - - - - - - -    - - - - - - - - - - - -   - -

      Unit 2

      Unit 3

      Unit 4

      Unit 5

      Unit 6

Hit <Space> to select: (U)ntagged, (T)agged, or (_) Not a Member
<ESC> Back                                      <Ctrl-L> Refresh  <Ctrl-W> Save
```



```
                        FSM726S Managed Stackable Switch
                                VLAN Membership

        VLAN ID:  5
      VLAN Name:  Sales

                                    1 1 1    1 1 1 1 1 1 1 2 2 2 2 2   2 2
      Port        1 2 3 4 5 6 7 8 9 0 1 2    3 4 5 6 7 8 9 0 1 2 3 4   5 6

      Unit 1      U - - U U - - - - - - -    - - - - - - - - - - - -   - -

      Unit 2

      Unit 3

      Unit 4

      Unit 5

      Unit 6

Hit <Space> to select: (U)ntagged, (T)agged, or (_) Not a Member
<ESC> Back                                      <Ctrl-L> Refresh  <Ctrl-W> Save
```



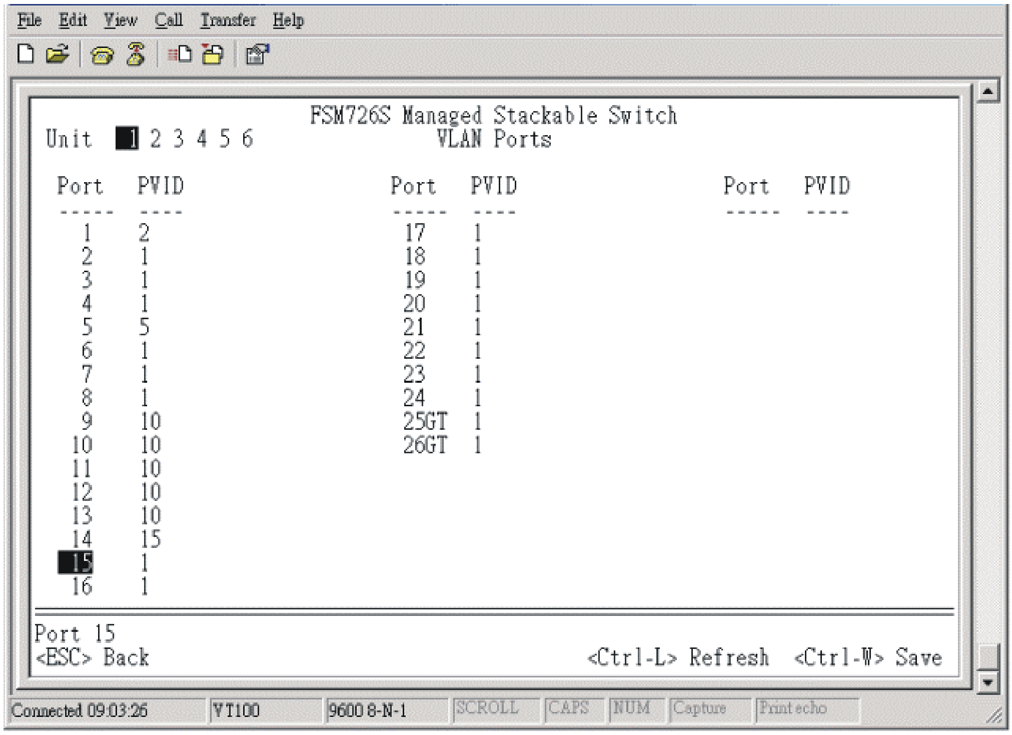
```
                  FSM726S Managed Stackable Switch
                          VLAN Membership

      VLAN ID:  10
    VLAN Name:  RD
                                  1 1 1   1 1 1 1 1 1 1 2 2 2 2 2   2 2
    Port        1 2 3 4 5 6 7 8 9 0 1 2   3 4 5 6 7 8 9 0 1 2 3 4   5 6

    Unit 1      T - - - - - - - T T U U   █ - - - - - - - - - - -   - -

    Unit 2

    Unit 3

    Unit 4

    Unit 5

    Unit 6

Hit <Space> to select: (U)ntagged, (T)agged, or (_) Not a Member
<ESC> Back                                  <Ctrl-L> Refresh  <Ctrl-W> Save
```



```
                  FSM726S Managed Stackable Switch
                          VLAN Membership

      VLAN ID:  15
    VLAN Name:  MIS
                                  1 1 1   1 1 1 1 1 1 1 2 2 2 2 2   2 2
    Port        1 2 3 4 5 6 7 8 9 0 1 2   3 4 5 6 7 8 9 0 1 2 3 4   5 6

    Unit 1      U U - - - - - - - - - -   - U - █ - - - - - - - -   - -

    Unit 2

    Unit 3

    Unit 4

    Unit 5

    Unit 6

Hit <Space> to select: (U)ntagged, (T)agged, or (_) Not a Member
<ESC> Back                                  <Ctrl-L> Refresh  <Ctrl-W> Save
```

3) Setup the Port VLAN IDs as follows.

Note: Port 01 PVID is set to 2. This must be done in the port specific page since there is no VLAN with ID 2



```
                         FSM726S Managed Stackable Switch
Unit  1 2 3 4 5 6                  VLAN Ports

 Port   PVID                     Port   PVID                     Port   PVID
 -----  ----                     -----  ----                     -----  ----
   1    2                         17    1
   2    1                         18    1
   3    1                         19    1
   4    1                         20    1
   5    5                         21    1
   6    1                         22    1
   7    1                         23    1
   8    1                         24    1
   9    10                        25GT  1
  10    10                        26GT  1
  11    10
  12    10
  13    10
  14    15
  15    1
  16    1

Port 15
<ESC> Back                                  <Ctrl-L> Refresh  <Ctrl-W> Save
```

The specific ports above have the following Port VLAN ID settings (The Port VLAN ID settings for each port are configured in the VLAN Ports page):

Port 01: 2	Port 05: 5	Port 09: 10	Port 13: 10
Port 02: 1	Port 06: 1	Port 10: 10	Port 14: 15
Port 03: 1	Port 07: 1	Port 11: 10	Port 15: 1
Port 04: 1	Port 08: 1	Port 12: 10	Port 16: 1

The following scenarios will produce results as described below:

1) If an untagged packet enters Port 4, the switch will tag it with a VLAN tag value of 1. Since Port 4 does not have membership with VLAN ID 1 (default), the packet will be dropped.

2) If a tagged packet with a VLAN tag value 5 enters Port 4, the packet will have access to Ports 5 and 1. If the packet leaves Port 5 and/or 1, it will be stripped of its tag becoming an untagged packet as it leaves the switch.

3) If an untagged packet enters Port 1, the switch will tag it with a VLAN tag value of 2. It will then be dropped since Port 1 has no membership with VLAN ID 2.

4) If a tagged packet with a VLAN tag value 10 enters Port 9, it will have access to Ports: 1, 10, 11, and 12. If the packets leave Ports 1 or 10, they will be tagged with a VLAN ID value of 10. If the packet leaves Ports 11 or 12, it will leave as an untagged packet.

5) If a tagged packet with a VLAN tag value 1 enters Port 9, it will be dropped since Port 9 does not have membership with VLAN ID 1.

APPENDIX D: TECHNICAL SPECIFICATIONS

This appendix provides technical specifications for the NETGEAR Model FSM726S Managed Stackable Switch.

Network Protocol and Standards Compatibility

IEEE 802.3 10BASE-T
IEEE 802.3u 100BASE-TX
IEEE 802.3z 1000BASE-SX
IEEE 802.3ab 1000BASE-T
IEEE 802.3x flow control

Management
IEEE 802.1Q Static VLAN (Up to 64)
IEEE 802.1p Class of Service (CoS)
IEEE 802.1D Spanning Tree Protocol
IEEE 802.1ad Link Aggregation Control Protocol (LACP)
IGMP v1, v2 Snooping Support
Port Mirroring support
SNMP v1
RFC1757 RMON groups 1,2,3, and 9
RFC1213 MIB II
RFC1643 Ethernet Interface MIB
RFC1493 Bridge MIB
Private Enterprise MIB

Interface
26 RJ-45 connectors for 10BASE-T, 100BASE-TX, and 1000BASE-T (Auto Uplink™ on all ports)
2 Gigabit Interface Converter (GBIC) slots for GBIC modules
RS-232 Console Port
2 Rear Stacking Connectors

LEDs
Per port (10/100 and Gigabit): Link, Speed, Duplex, Activity, Collision
Per device: Power, Stack, Master

Performance Specifications
Forwarding modes: Store-and-forward
Bandwidth: 12.8 Gbps (Non-blocking)
Network latency: Less than 80 microseconds for 64-byte frames in store-and-forward mode for10 Mbps to 100 Mbps transmission
10/100 buffer memory: 735 KB embedded memory for 24 ports
Gigabit buffer memory: 122 KB embedded memory per port
Address database size: 8,000 media access control (MAC) addresses per system
Addressing: 48-bit MAC address
Acoustic noise: (ANSI-S10.12) 45 dB
Heat Dissipation: 18.99 Btu/hr
Mean Time Between Failure (MTBF): 58,300 hours (~ 6.5 years)

Power Supply
Power Consumption: 36 W maximum
100-240VAC/50-60 Hz universal input

Physical Dimensions
440 x 253 x 43 mm (W x D x H)
17.32 x 9.96 x 1.7 inch

Environmental Specifications
Operating temperature: 0 to 40°C
Storage temperature: -20 to 70°C
Operating humidity: 90% maximum relative humidity, non-condensing
Storage humidity: 95% maximum relative humidity, non-condensing
Operating altitude: 10,000 ft (3,000 m) maximum
Storage altitude: 10,000 ft (3,000 m) maximum

Electromagnetic Emissions
CE mark, commercial
FCC Part 15 Class A
VCCI Class A
EN 55022 (CISPR 22), Class A
C-Tick

Electromagnetic Immunity
EN 50082-1
EN 55024

Safety
CE mark, commercial
CSA certified (CSA 22.2 #950)
TUV licensed (EN 60 950)
UL listed (UL 1950)/cUL IEC950/EN60950

Modules
AGM721F GBIC SX module for 1000BASE-SX connection with SC connectors for 50um or 62.5um multi-mode fiber cable

APPENDIX E: CONNECTOR PIN ASSIGNMENTS

This appendix provides information about the RJ-45 plug and the RJ-45 connector used for the NETGEAR Model FSM726S Managed Stackable Switch.

RJ-45 Plug and RJ-45 Connector

In a Fast Ethernet network, it is important that all 100BASE-T certified Category 5 cabling use RJ-45 plugs. The RJ-45 plug accepts 4-pair UTP or shielded twisted-pair (STP) 100-ohm cable and connects into the RJ-45 connector. The RJ-45 connector is used to connect stations, hubs, and switches through UTP cable; it supports 10 Mbps, 100 Mbps, or 1000 Mbps data transmission.
Figure E-1 shows the RJ-45 plug and RJ-45 connector.

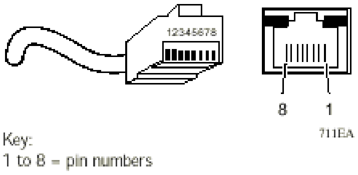


Figure E-1. RJ-45 Plug and RJ-45 Connector with Built-in LEDs

Table E-1 lists the pin assignments for the 10/100 Mbps RJ-45 plug and the RJ-45 connector.

Table E-1. 10/100 Mbps RJ-45 Plug and RJ-45 Connector Pin Assignments

Pin	Normal Assignment on Ports 1 to 8	Uplink Assignment on Port 8
1	Input Receive Data +	Output Transmit Data +
2	Input Receive Data –	Output Transmit Data –
3	Output Transmit Data +	Input Receive Data +
6	Output Transmit Data –	Input Receive Data –
4, 5, 7, 8	Internal termination, not used for data transmission	

Table E-2 lists the pin assignments for the 100/1000 Mbps RJ-45 plug and the RJ-45 connector.

Table E-2. 100/1000 Mbps RJ-45 Plug and RJ-45 Connector Pin Assignments

Pin	Channel	Description
1 2	A	Rx/Tx Data + Rx/Tx Data
3 6	B	Rx/Tx Data + Rx/Tx Data
4 5	C	Rx/Tx Data + Rx/Tx Data
7 8	D	Rx/Tx Data + Rx/Tx Data

APPENDIX F: CABLING GUIDELINES

This appendix provides specifications for cables used with the NETGEAR Model FSM726S Managed Stackable Switch.

Fast Ethernet Cable Guidelines

Fast Ethernet uses UTP cable, as specified in the IEEE 802.3u standard for 100BASE-TX.The specification requires Category 5 UTP cable consisting of either two-pair or four-pair twisted insulated copper conductors bound in a single plastic sheath. Category 5 cable is certified up to 100 MHz bandwidth. 100BASE-TX operation uses one pair of wires for transmission and the other pair for receiving and for collision detection.
When installing Category 5 UTP cabling, use the following guidelines to ensure that your cables perform to the following specifications:

Certification
Make sure that your Category 5 UTP cable has completed the Underwriters' Laboratories (UL) or Electronic Testing Laboratories (ETL) certification process.

Termination method
To minimize cross-talk noise, maintain the twist ratio of the cable up to the point of termination; untwist at any RJ-45 plug or patch panel should not exceed 0.5 inch (1.5 cm).

Category 5 Cable

Category 5 distributed cable that meets ANSI/EIA/TIA-568-A building wiring standards can be a maximum of 328 feet (ft) or 100 meters (m) in length, divided as follows:

20 ft (6 m) between the hub and the patch panel (if used)

295 ft (90 m) from the wiring closet to the wall outlet

10 ft (3 m) from the wall outlet to the desktop device

The patch panel and other connecting hardware must meet the requirements for 100 Mbps operation (Category 5). Only 0.5 inch (1.5 cm) of untwist in the wire pair is allowed at any termination point.

Category 5 Cable Specifications

Ensure that the fiber cable is crossed over to guarantee link.
Table F-1 lists the electrical requirements of Category 5 UTP cable.

Table F-1. Electrical Requirements of Category 5 Cable

Specifications	Category 5 Cable Requirements
Number of pairs	Four
Impedance	100 Ω ± 15%
Mutual capacitance at 1 KHz	≤5.6 nF per 100 m
Maximum attenuation (dB per 100 m, at 20° C)	at 4 MHz: 8.2 at 31 MHz: 11.7 at 100 MHz: 22.0
NEXT loss (dB minimum)	at 16 MHz: 44 at 31 MHz: 39 at 100 MHz: 32

Twisted Pair Cables

For two devices to communicate, the transmitter of each device must be connected to the receiver of the other device. The crossover function is usually implemented internally as part of the circuitry in the device. Computers and workstation adapter cards are usually media-dependent interface ports, called MDI or uplink ports. Most repeaters and switch ports are configured as media-dependent interfaces with built-in crossover ports, called MDI-X or normal ports. Auto Uplink technology automatically senses which connection, MDI or MDI-X, is needed and makes the right connection.

Figure F-1 illustrates straight-through twisted pair cable.

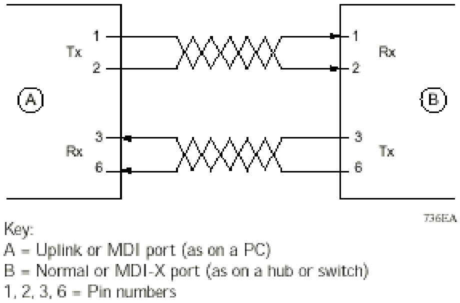

1
Tx
2
A
3
Rx
6
1
Rx
2
B
3
Tx
6
736EA
Key:
A = Uplink or MDI port (as on a PC)
B = Normal or MDI-X port (as on a hub or switch)
1, 2, 3, 6 = Pin numbers

Figure F-1. Straight-Through Twisted-Pair Cable

Figure F-2 illustrates crossover twisted pair cable.

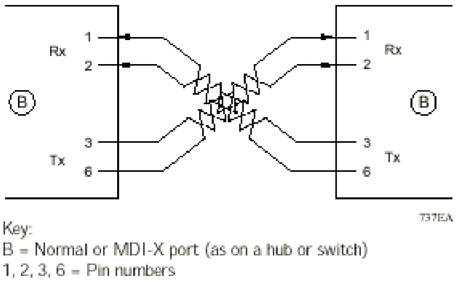


Figure F-2. Crossover Twisted-Pair Cable

Patch Panels and Cables

If you are using patch panels, make sure that they meet the 100BASE-TX requirements. NETGEAR recommends Category 5 UTP cable for all patch cables and work area cables to ensure that your UTP patch cable rating meets or exceeds the distribution cable rating.
To wire patch panels, you need two Category 5 UTP cables with an RJ-45 plug at each end, as shown in Figure F-3.

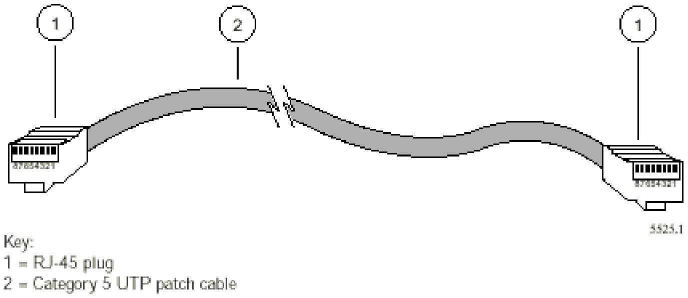


Figure F-3. Category 5 UTP Cable with Male RJ-45 Plug at Each End

Note: Flat “silver satin” telephone cable may have the same RJ-45 plug. However, using telephone cable results in excessive collisions, causing the attached port to be partitioned or disconnected from the network.

Using 1000BASE-T Gigabit Ethernet over Category 5 Cable

Overview

When using the new 1000BASE-T standard, the limitations of cable installations and the steps necessary to ensure optimum performance must be considered. The most important components in your cabling system are patch panel connections, twists of the pairs at connector transition points, the jacket around the twisted-pair cable, bundling of multiple pairs on horizontal runs and punch down blocks. All of these factors affect the performance of 1000BASE-T technology if not correctly implemented. The following sections are designed to act as a guide to correct cabling for 1000BASE-T.

Cabling

The 1000BASE-T product is designed to operate over Category 5 cabling. To further enhance the operation, the cabling standards have been amended. The latest standard is Category 5e, which defines a higher level of link performance than is available with Category 5 cable.
If installing new cable, we recommend using Category 5e cable, since it costs about the same as Category 5 cable. If using the existing cable, be sure to have the cable plant tested by a professional who can verify that it meets or exceeds either ANSI/EIA/TIA-568-A:1995 or ISO/IEC 11801:1995 Category 5 specifications.

Length

The maximum distance limitation between two pieces of equipment is 100 m, as per the original Ethernet specification. The end-to-end link is called the "channel."
TSB-67 defines the "Basic Link" which is the portion of the link that is part of the building infrastructure. This excludes patch and equipment cords. The maximum basic link length is 295 feet (90 m).

Return Loss

Return loss measures the amount of reflected signal energy resulting from impedance changes in the cabling link. The nature of 1000BASE-T renders this measurement very important; if too much energy is reflected back on to the receiver, the device does not perform optimally.
Unlike 10BASE-T and 100BASE-TX, which use only two of the four pairs of wires within the Category 5, 1000BASE-T uses all four pairs of the twisted pair. Make sure all wires are tested — this is important.

Factors that affect the return loss are:

The number of transition points, as there is a connection via an RJ-45 to another connector, a patch panel, or device at each transition point.

Removing the jacket that surrounds the four pairs of twisted cable. It is highly recommended that, when RJ-45 connections are made, this is minimized to 1-1/4 inch (32 mm).

Untwisting any pair of the twisted-pair cabling. It is important that any untwisting be minimized to 3/8 inch (10 mm) for RJ-45 connections.

Cabling or bundling of multiple Category 5 cables. This is regulated by ANSI/EIA/TIA-568A-3. If not correctly implemented, this can adversely affect all cabling parameters.

Near End Cross Talk (NEXT)

This is a measure of the signal coupling from one wire to another, within a cable assembly, or among cables within a bundle. NEXT measures the amount of cross-talk disturbance energy that is detected at the near end of the link — the end where the transmitter is located. NEXT measures the amount of energy that is "returned" to the sender end. The factors that affect NEXT and cross talk are exactly the same as outlined in the Return Loss section. The cross-talk performance is directly related to the quality of the cable installation.

Patch Cables

When installing your equipment, replace old patch panel cables that do not meet Category 5e specifications. As pointed out in the NEXT section, this near end piece of cable is critical for successful operation.

Conclusion

For optimum performance of your 1000BASE-T product, it is important to fully qualify your cable installation and ensure it meets or exceeds ANSI/EIA/TIA-568-A:1995 or ISO/IEC 11801:1995 Category 5 specifications. Install Category 5e cable where possible, including patch panel cables. Minimize transition points, jacket removal, and untwist lengths. Bundling of cables must be properly installed to meet the requirements in ANSI/EIA/TIA-568A-3.

NETGEAR, Inc.
4500 Great America Parkway
Santa Clara, CA 95054 USA
Phone: 1-888-NETGEAR
www.NETGEAR.com
February 2002 M1-FS726SNA-0